~~TOP SECRET~~

DF-112
IF-294-C

27/48/TOPSEC/AS-14-Ticom

Survey of Russian Military Systems.

1. The attached is an Army Security Agency translation of a paper by Alex Dettmann, former Lieutenant in the German Army and officer-in-charge of the Russian section of the Signal Intelligence Agency of the German Army High Command (OKH/GdNA/In 7/VI). It was received by Army Security Agency through non-TICOM channels.

2. The paper was written by Dettmann over a period of several months in 1947. Although written entirely from memory it gives a comprehensive picture of the history of the German Army cryptanalytic effort against Russian Army, Air and NKVD systems.

3. The present paper is a fuller discussion than that presented in the previous review of the same field written for TICOM by Dettmann and his chief assistant, Samsonoff (available as TICOM Document 805) or the descriptive summary written by Dettmann shortly before V-E Day and found in the archives of In 7/VI (TICOM Document 2765, translated as DF-94). Dettmann states (page 2) that he wrote another paper on this subject for the British but of this Army Security Agency has no further knowledge.

4. The present paper has interest from an administrative and historical point of view but unfortunately many topics of potential operational interest are "reserved for a subsequent paper." Two outlines and a section of text (see Supplement) may belong to this proposed study.

30 copies:

Translated: R.W.P.
1 April 1948

266 pages

Distribution:

1	AS-10, AS-23, AS-14 file
2	AS-70, AS-76-C file
3	AS-80, AS-83 file
4	AS-90, AS-96 file
5-7	CSAW
8-9	LSIC
10	CSGID
11	CSO
12	ASA/Europe
13	AS-95
14-17	AS-93-B
18	AS-94
19	ASA/School, Officers training division
20-30	TICOM-file

~~EXEMPT~~
~~Classified/Extended by DIRNSA/CHCSS~~
~~Reason: NSA Declassification Guidelines~~
~~Re-Review on 27 July 2012~~
Date

Do NOT Destroy Return to the NSA Technical Library when no longer needed
S-3762
Copy No. 2

~~TOP SECRET~~

~~TOP SECRET~~

Complete table of contents to report:

"Cryptanalysis of Russian Traffic in the former German Army".
To permit checking the completeness of the material supplied.

	Original	ASA Pagination
Complete table of contents	1 sheet	1
Preface (pages 1--4)	4 sheets	2
Part I (evaluation of content)		
Introduction (page 5)	1 sheet	7
The General significance of the NKVD organs and their functions in peace and in war (pages 6 to 18)	13 sheets	8
Army and airforce (pages 19 to 30)	12 sheets	23
Intelligence results from decipherment of messages of the army, air force NKVD, partisan's and agent's radio	16 sheets	37
Part 2 (Technical part)	1 sheet	55
Introduction (page 47)		
Russian cryptography, structure and organization (pages 48--61)	14 sheets	56
Development of Russian military and political cryptographic systems in the light of cryptanalysis (pages 62--87)	26 sheets	71
Part 3 Development of cryptanalysis of Russian traffic in the former German army and criticism of organizational defects. (pages 88--105)	18 sheets	99
Part 4 (Appendix)		
Introduction	1 sheet	119
Table of contents of the appendix	2 sheets	120
1 page supplements: 1a,1b--1c--1d,1e--1f--2--3--4--4a--5 5a--6--6a--7--7a--8--8a--9--9a--10-- 10a--11--11a--12--12a--13--13a--14-- 14a--15--15a--16--16a--17--18a--18b-- 18c--18d--19--19a--23--24--25--26	43 sheets	
Appendix 20 Glossary of terms	4 sheets	166
" 21 Listing of pre-war systems	15 sheets	170
22 Listing of war time systems	13 sheets	187
Total	184 sheets	
Supplement: Cryptographic and Cryptanalytic Aids		201

~~TOP SECRET~~

~~TOP SECRET~~

Preface

The third and final form of the report on the cryptanalysis of Russian traffic in the former German army is based on other complete studies by the author and the former two reports, of which the first -- written in American captivity from June to August 1945, was turned over to Major Bundy SIS USFET Headquarters -- Hüsselheim in August 1945, and the second, considerably more complete report, was written from February to March 1946 in Lübeck after release from captivity and was delivered to the British office "Royal Signals" and 2 S.A.I.O., Lübeck, in April 1946. On the basis of the second report and of his knowledge in the Signal Intelligence Field for Russia the author was at the disposition of the British office from 10 January to 10 May 1945, but was not regularly employed, and on the advice of the director of this office, Mr. Uff, placed himself at the disposal of the appropriate US office in June 1947.

The author of this report is the former Chief Analyst and sometime Section Chief (Russia) of the "General der Nachrichtenaufklärung," the guiding central office for the Signal Intelligence Service in the former German army. This central office with the OKH -- Chef HNW (Oberkommando des Heeres -- Chef Heeres Nachrichtenwesen) came into being in the spring of 1939. Up to this time all Signal Intelligence was subordinate in its technical aspects to the OKW; after attachment to the army the fields of competence were separated. The army took over work on all military or political systems, while OKW was to occupy itself exclusively with diplomatic ciphers. Changes in the structure of the controlling office, the development of signal intelligence in general and the events of the war

resulted in several changes in the name of the central office during the war years. Finally recognition of the importance and ever increasing significance of Signal Intelligence led, even though very late, to the separation of signal intelligence from the general signal service and its subordination to a general officer of its own. Thus out of the former "Oberleitstelle" (1939-41) came the "Leitstelle der Nachrichten-Aufklärung" (1941-44) and finally the office of the "General der Nachrichten-Aufklärung" (1944-1945). The author was active from 1935, i. e. practically from the beginning of any systematic monitoring of Russia by Germany, as scientific collaborator in the field of Russian cryptanalysis, from 1935 to 1939 at the fixed radio receiving stations (or intercept stations) Jüterbog and Treuenbrietzen, at first as analyst and translator, later as chief analyst and section head; from 1939 to 1945 at the control office as chief analyst and teacher, temporarily as section head and director of a mechanical work shop for analytic aids. He may therefore be regarded as the only person fully competent in the field of analysis of all military and political systems. On the basis of his long experience and practice in an administrative capacity, but in particular due to his practically uninterrupted employment in all parts of this field, the author is the only person in Germany who is in a position to compose a report analyzing all Russian military and political cryptographic systems with respect to the possibility of decipherment.

Aside from the author there are without question a number of important analysts in the field of Russian, some of whom worked with the same outfit under the author or in the outstations. In contrast to the author of this report however, these persons were used for limited analytic assignments and

hence do not have a comprehensive acquaintance with all fields of cryptanalysis of Russian traffic or in the course of the years were entrusted with other tasks.

As guiding force of the analytic organization the author is also in a position to give a dependable picture of the value of evaluation of the deciphered material, all the more since the evaluation down to 1939 was made by the analyst himself and represents nothing more than a sorting, collecting and practical utilization of the final results of decipherment. Of course there is no question but that the real evaluation of content, i. e. the deductions from the deciphered material as to intentions, measures and plans of the enemy, does not belong within the framework of cryptanalysis but must be a task for officers of the General Staff, on the other hand the status in the German army since 1939, where subordinate officials or young inexperienced officers without linguistic knowledge tried their hand at evaluation, is decried. Close contact between cryptanalysis and evaluation of content must be maintained and above all the results, inferences and the combined enemy situation must always be available to the analyst.

It can be asserted that the plaintexts derived from deciphered messages are always absolutely reliable and often very important communications since the enemy dispatches them for his own use and uses simple, complicated or exceedingly difficult methods of encipherment according to whether they are "secret for the time being", "secret" or "strictly secret."

Other sources of intelligence available to the high command — reports of agents, statements of deserters and prisoners, observations of the air force and other reconnaissance reports cannot compete with the results of cryptanalysis since, being subject to individual human weaknesses, deception of the senses or other influences, they are often consciously or unconsciously defective, sometimes even false. Insofar as there may be any need of confirmation of the assertion respecting the reliability of decipherments as a source of intelligence, we may point to the fact that in innumerable cases these reports were subsequently confirmed by captured material, by interrogation of prisoners and by reports of agents. Furthermore the events forecast by the decipherment of enemy radiograms always occurred, observations of all sorts such as displacements [troop movements], conditions and situations which were made possible by cryptanalytic have always proven correct where it was possible to check. Consequently the results of decipherment in the form of translated text were also designated and evaluated by the high command as "Verlässliche Nachrichten" (V.N.). These "dependable communications" yielded 90% of the basis for all enemy situation reports, among others the so called "red situation chart", and were treated according to their content as "secret" or "top secret". Aside from these "Verlässlichen Nachrichten" two other types of reports were issued daily by the control station and delivered to the highest command either "by telephone in advance" or by courier according to their importance. These were the "radio situation report", a report on operational and traffic evaluation giving results and deductions from the traffic, nets and radio stations observed, monitored and

located. The biggest report by far was the so called "intercept situation" a product of content evaluation based on the final results of decipherment, traffic analysis, telephonic reports of out-stations and information from air force cryptanalysis and/or the allied Finnish cryptanalytic central office. That the significance of this report was unfortunately often problematic was due to the inadequate staffing of the evaluation section, not in a quantitive but in a qualitative way. (see part III)

The cryptanalytic organization of OKH which was directed by the author was able to supply the supreme command with important and ultra important information up to the final phase of the war. Due to lack of military potential, operational and tactical utilization of these reports could not be made toward the last.

Part I

(Content evaluation)

As already mentioned in the Preface, content evaluation, if not a part of cryptanalysis as originally assumed, is nevertheless an immediately adjacent field and completely dependent on decipherment. It should not cause surprise that in this report -- cryptanalysis of Russian traffic in the former German army — the subject of evaluation is taken up first since in contrast to cryptanalysis -- in particular to the technical analysis of cipher systems -- it represents a generally comprehensible field and the great value of importance of a decipherment can only be derived from its conclusions, the assembled, sorted, correctly and definitively evaluated deciphered texts. If under content evaluation the NKVD (НАРОДНЫЙ КОММИССАРИАТ ВНУТРЕННЫХ ДЕЛ = Peoples Commissariat for Internal Affairs) and its organs are described first, this is due to the fact that precisely this organization first used radio as a means of communication and developed it beyond the practice stage for its own purposes. In the years 1935/1936 approximately 70% of all intercepted radiograms, as far as these could be deciphered, were communications of NKVD organs.

Quite apart from this fact two other factors warrant preferential treatment of the NKVD systems. In the first place the NKVD systems used were long term cryptographic systems, i. e. used for a long time and consequently far more capable of development than the initially very short lived through simple systems of the army and air force. In the second place the content of the NKVD cipher messages was usually more interesting,

~~TOP SECRET~~

above all there was a desire to clear up the great unknowns NKVD and
GPU (ГОСУДАРСТВЕННОЕ ПОЛИТ. УПРАВЛЕНИЕ
= state political administration — this and the designation "tscheka"[cheka]
= Ч.К. = ЧРЕЗВЫЧАЙНАЯ КОММИССИЯ
= extraordinary commission have not been used since 1938).

The general significance of the NKVD organs and their functions in peacetime and war.

1. The NKVD as political security organ.
2. The NKVD as rampart against the outside world.
3. The NKVD as organ of economic control.
4. The NKVD and the RKKA
   a. The NKVD as control organ.
   b. The NKVD as training organ.
   c. The NKVD as elite troops.
5. Additional assignments of NKVD in time of war.

Among the first successes of the decipherment of Russian secret messages belongs the recognition of the significance of NKVD in the political, military and economic life of the Soviet Union. It soon became apparent that the role of this organization was far more comprehensive and that it exerted much stronger influence on military affairs than had previously been assumed. These discoveries caused the utmost attention to be devoted to monitoring the radio traffic of the NKVD. The basic task of the NKVD is to assure the continuation of the political structure of the USSR, among [illegible] of Bolshevist ideas, combating by rigorous means

~~TOP SECRET~~

the freely expressed opinions of those who think otherwise, and an intensive proproganda which negates all else; hence it exercises the sharpest control over the political, military and economic life of the country. For this purpose there are set up administrative offices in every city of the country, in their structure these offices correspond to the manifold tasks assigned them. To carry out the necessary measures the NKVD has at its disposal its own contingents of troops of various categories, NKVD troops, which are allocated and assigned by the central office in Moscow, the GUP = ГУП ВОЙСК НКВД - ГЛАВНОЕ УПРАВЛЕНИЕ ВОЙСК НКВД = main administration of NKVD troops, according to need.

The duties of political supervision are performed by the ПОЛИТ ОТДЕЛЫ НКВД = political sections of the NKVD with the aid of an extensive network of agents through which every movement hostile to the Soviets can be recorded and combatted. For the later purpose the NKVD uses contingents of troops called ВНУТРЕННИЕ ВОЙСКА = interior troops.

Members of this force, if we can speak of such a thing, are in the lower service grades almost exclusively civilians in all sorts of occupations, young people and a very large number of women. This system of informers, which is very wide spread had been developed since the days of the Czarist ОХРАНА = security service, refined and greatly strengthened in all levels of the population, is the sure guarantee of the carrying out of Bolshevick wishes out of fear of what might happen to those nearest you. With the occupation of foreign territory in the course of

~~TOP SECRET~~

this war the number of political sections grew very materially, because the occupied areas required a more intensified surveillance due to an often essentially different political structure. As a result the contingents of internal troops had to be materially increased.

The sending away of politically undependable elements, the guarding and administration of concentration camps, the employment of penal work camps and penal battalions and the transportation to the rear of prisoners of war as well as guarding them there, these belong to the duties of the КОНВОЙНЫЕ ВОЙСКА НКВД = escort troops NKVD.

Corresponding to the special political structure of the USSR, in particular to the combating of all foreign ideological influences, provision had to be made for sealing off the country in almost hermetic fashion from the adjacent foreign countries. This gave occassion for the creation of an effective and dependable border guard which was taken over by the ПОГРАНИЧНЫЕ ВОЙСКА = the border and security troops NKVD. Only those frontier areas of slight extent or thinly populated and generally impassable and hence easy to watch were originally turned over to the army. Since the beginning of 1939 however even these stretches have been guarded by the NKVD border troops. Corresponding to their assignments these NKVD troops have at their disposal airplanes and, where water boundaries are involved, aquaplanes and surface craft ranging from motor boats and steam cutters to speed boats and gun boats. As early as 1935 — 1937 decipherment of messages from several Russian border guard areas gave away the structure, duties, effectiveness and strength of the units.

~~TOP SECRET~~

Thus we could read currently traffic of the border and coast guard areas:

1. North/Control station Murmansk.
   Petshora to the Finnish frontier.

2. Leningrad/Control station Leningrad
   Karelian peninsula and Finnish frontier.

3. Odessa/Control station Odessa
   Bessarabia to the east coast of Crimea

4. Novorossijsk/Control station Novorossijsk
   Coastal area Sea of Azov and the northwest coast of the Black Sea.

5. Transcaucasus/Control stations Sukhum and Baku
   East coast of the Black Sea, Turkish border and that with Iran and the West coast of the Caspian Sea.

6. Kasakhstan/Control stations Tashkent and Alma Ata, East coast of the Caspian Sea and the frontier toward other Asiatic countries.

The first four of the above named border guard areas, at that time subordinated to the so called UPVO NKVD (УПРАВЛЕНИЕ ПОГРАНИЧНОГО ВОЕННОГО ОКРУГА = administration of the frontier district NKVD) in Moscow, each had one border guard battalion, the last two had two border guard battalions each (formerly called ДИВИЗИОН, later ОТДЕЛЕНИЕ), which in their strength corresponded approximately to a reenforced regiment and which were made up of a number of sub-sections (ОТРЯДЫ) according to the geographic situation. These sub-sections on their part are divided into border or coast detachments which set up border or coast posts of various strength which actually attended to blocking the frontier. In later years it was learned that the organization of the border guard was the same in the Far East.

~~TOP SECRET~~

The service in these border and coast patrol battalions was set up in a completely military fashion but was in no wise comparable with that of the RKKA (РККА= РАБОЧАЯ КРЕСТЬЯНСКАЯ КРАСНАЯ АРМИЯ = red worker and peasant army). Along with pure police functions the members of these NKVD units also performed the duties of customs officials and political police and included in their ranks experienced seaman and pilot s. Great importance especially in the case of officers attached to the mastery of foreign languages. It can be stated that the level of officers and men was exceptionally high and that these troops of the NKVD were justly designated as an elite body.

The map sections given in appendix 1a-f (part IV) showing the areas where the above units were employed make no claim to completion since the period when this traffic was observed lies a long way back and the data can only be derived from memory.

From current monitoring of the radio traffic of the border guard units it developed that with the beginning of the war the organization of the border guard facing hostile countries underwent a basic change. Aside from an extensive adjustment of the structure of the border troops NKVD to that of the RKKA (division into regiments and battalions), the assignments also changed materially. It was soon ascertained that by the use of regiments of the NKVD border troops a continuous, very mobile and deep echeloned security girdle had been set up at a distance of 30 to 60 kilometers behind the fighting troops of the RKKA. Of approximately 200 border guard regiments recognized by cryptanalysis approximately 1/3 was recognized as the front line of the security belt, while the second third was employed farther back and the final third formed a mobile reserve. Each of the regiments of the front line guarded

~~TOP SECRET~~

an area up to 60 kilometers wide. In the course of time it could be shown that to secure the rear area of an army of the RKKA, independent of the width of the front, 1 or 2 NKVD regiments would be required. Determination of the employment of these regiments was made by front staff of the NKVD itself, these were in the immediate vacinity of, often in the same place with the front staff of the army but got their orders from the NKVD central office in Moscow. To a front sector, of which after the capitulation of Findland there were about 11, there were assigned 5 to 8 NKVD border guard regiments for the first line of the security belt. The task of this belt was to prevent desertion and the penetration of hostile agents into the interior by hermetically sealing off the front area from the zone of communicatio s, to clear areas near the front of enemy groups and bands which had become separated, and to remove the population to a depth of 20 to 30 kilometers, to remove and resettle for political considerations, to employ the population for repair and rebuilding of roads, defenses, air fields and economic plants, to guard replacements on the roads([?] Rollbahnen)and to assemble and transport prisoners to the interior. After the occupation of German territory by the RKKA and the penetration of the area by NKVD organs which followed shortly thereafter, an additional very important task was turned over to the border troops NKVD. This was seizing all men left in the area between 14 and 65 and all women between 14 and 50 who were capable of work and getting them ready to be carried away. Down into May 1945 we could read currently orders regarding the making up of such transports, instructions for feeding and assignment of personnel, arrangements for punishments to be imposed, such as beating, shooting or simply liquidation of those who did not step lively, and reports of the execution of such orders. The great number of

tasks to be accomplished made it necessary to reenforce the security belt by additional NKVD regiments, in particular where rather large encircled enemy troop units were still putting up successful resistance behind the Russians' own front and employment of the NKVD troop was possible. Likewise it was necessary to keep the occupied rear area completely under control, the contingents of interior troops did not suffice for this, often they lacked the military experience, hence for this purpose also additional NKVD regiments were required. The number of border regiments employed for the security girdle, which in the period from autumn 1943 to the winter of 1944 ran about 60 to 75, may have reached about 100 by the date of the capitulation.

Of decisive importance for our evaluation was the fact that the NKVD border guard regiment remained in constant coordinated relation with the army of the RKKA they were supposed to safeguard, i. e. in case of change of position, say from one wing of the front to the other or even from one front to another, these regiments moved with the army. Hence it was possible to check the location of armies of the RKKA and so concentrations, shifts of strength, and creation of strong points by observing the traffic of these border guard units.

The change in structure of the border guard units and their composition before and during the war can best be shown by the following comparison:

Before 1942 Battalion	Number in each battalion	Since 1942 Regiment	Number in each regiment
Sub-battalion [commandantur?]	3—5	Battalion	3
Outpost	various	Outpost	9
		Reserve outpost	Up to 3
Detachments		[illegible]	various
		operative group	various

an area up to 60 kilometers wide. In the course of time it could be shown that to secure the rear area of an army of the RKKA, independent of the width of the front, 1 or 2 NKVD regiments would be required. Determination of the employment of these regiments was made by front staff of the NKVD itself, these were in the immediate vacinity of, often in the same place with the front staff of the army but got their orders from the NKVD central office in Moscow. To a front sector, of which after the capitulation of Findland there were about 11, there were assigned 5 to 8 NKVD border guard regiments for the first line of the security belt. The task of this belt was to prevent desertion and the penetration of hostile agents into the interior by hermetically sealing off the front area from the zone of communicatio s, to clear areas near the front of enemy groups and bands which had become separated, and to remove the population to a depth of 20 to 30 kilometers, to remove and resettle for political considerations, to employ the population for repair and rebuilding of roads, defenses, air fields and economic plants, to guard replacements on the roads([?] Rollbahnen) and to assemble and transport prisoners to the interior. After the occupation of German territory by the RKKA and the penetration of the area by NKVD organs which followed shortly thereafter, an additional very important task was turned over to the border troops NKVD. This was seizing all men left in the area between 14 and 65 and all women between 14 and 50 who were capable of work and getting them ready to be carried away. Down into May 1945 we could read currently orders regarding the making up of such transports, instructions for feeding and assignment of personnel, arrangements for punishments to be imposed, such as beating, shooting or simply liquidation of those who did not step lively, and reports of the execution of such orders. The great number of

Note: The outposts are numbered 1 to 9 (or 12) within a regiment.

Compare appendix 2 (part IV) area of employment of an NKVD regiment.

Among the successes of our cryptanalysis belongs also the early establishment of the fact that the entire economy of the Soviet Union, particularly military economy and communications system, are under very rigid control and so under the influence of the NKVD. For this purpose the NKVD employed the local units of its interior troops. These supervise constantly the carrying out of tasks set by the state planned economy and make regular reports to their superior offices. Decipherment made possible the reading of such control reports and afforded hints as to the capacity of many branches of economic importance, often showed unsatisfactory conditions and the methods used to combat and eliminate these. Such reports were especially valuable during the war since they allowed us to recognize the kind and extent of the difficulties with which economic leadership of the Soviet Union had to contend. In the course of the war the functions of these NKVD offices was expanded in as much as along with intensification of the peace time controls and their right to intervene directly when bad conditions arose, they were assigned the task of putting into operation closed or destroyed economic plants as well as that of building new ones. For this purpose the officers of the interior troops of the NKVD mustered all technical persons in their areas and put them to work or in case of need sent them to other NKVD areas. These duties became especially comprehensive with the territorial expanse resulting from the occupation of new territory in the west and, as already mentioned, could only be carried out with the support of the border and security troops of

the NKVD.

As an essential part of the entire economy of the country the communication system, in particular rail traffic, was under the control of the NKVD. After the outbreak of the war protection of the railroads had to be taken over along with the control. This called for guarding transports, depots, bridges, junction points and important or endangered rail lines. To accomplish these tasks specially trained contingents ЖЕЛЕЗНОДОРОЖНЫЕ ВОЙСКА НКВД = railway troops NKVD were set up. The organization here corresponded to that of the army with the division as the largest unit. In areas near the front three divisions of NKVD railway troops were identified during the war and their employment could be followed currently. The NKVD railway troops are doubtless a war phenomenon like the NKVD convoy troops. These tasks in peace time fell in the sphere of activity of the interior troops, probably the troop contingents of these special units were set up about the turn of the year 1942/43. The insecurity on the railroads, especially close to the front, must have been very great around the beginning of 1943, to judge by decipherments. As numerous cases show, not only thieving was involved but wholesale robbery, murder and regular high-jacking. Above all in the Ukrain the Ukrain National Partisan groups were very active even after security on the railways had been generally increased by the use of railway troops NKVD and these Partisans endangered Russian transport to the front.

Since the main task of cryptanalysis in the former German army lay in clearing up military and political matters and messages of an economic character did not fall within the immediate assignment and could only be treated secondarily, the influence of the NKVD on economics could only be

recognized in a fragmentary fashion, but even thus the extremely important role of the NKVD in the economic life of the Soviet Union could be clearly recognized. Without a question a still wider influence of the NKVD on economic life would appear if the economic internal radio traffic were monitored fully and if it proved practicable to decipher the same.

Especially illuminating for any estimate of the power of the NKVD is the relation of this organization to the RKKA. The NKVD has taken over the political indoctrination of the RKKA, beginning with the General Staff and ending with the last private, in order to guarantee an absolutely Bolshevistic, Communistic philosophy in every member of the Red Army. For this purpose the NKVD has a system of political leadership and guidance extending from the General Staff down into the platoon of the company. By the use of the so called "fifth sections" (особый отдел = special section or политотдел = political section) in all staffs from the General Staff down to the Divisional Staff, and of политком = political commissar and политрук = political leaders in the lower formations to the platoon, every man is watched, guided and trained by the NKVD. Aside from the official representative of the NKVD mentioned above, secret agents and spies from the ranks of the Red army itself cooperate, it is the task of these later to recognize currents hostile to the Soviets among the leaders and troops in an early state and to report the same. Arrest and punishment are exclusively in the hands of military tribunals directed by the NKVD. The NKVD exercises a tremendous influence on the make up of the RKKA due to the fact that all changes in the ranks of the highest and

down to the medium command, as well as the selection and training of command replacements, can only be made with the consent of its organs.

Aside from the political education the NKVD was also charged with the military education of the RKKA in a number of special fields. Among others for instance training of sharp shooter units is handled by organs of the NKVD, which also runs schools for messenger dogs and messenger pigeons and has charge of the military toughening up of the youth of the land.

The largest sharp shooter units are regiments which can be broken up according to need into battalions, companies, platoons, groups, or individual marksmen and assigned to individual units of the RKKA. Since the sharp shooters in their frequent shifts from unit to unit are exposed to all sorts of whisperings and temptations and because they are often employed with badly depleted demoralized units and whereever they go almost always have isolated posts, it is not strange that the NKVD has taken charge and looked out for the proper training of these specialists.

A specially dangerous field is the safeguarding of military secrets. Hence it is quite comprehensible that the NKVD has been and is exceedingly active in this field. The security of Signals communications depends primarily on the dependability of the personnel entrusted therewith. For this reason the NKVD devotes particular attention to this group. In addition to selection and supervision of the technical communications personnel, the NKVD exercises the sharpest sifting and constant supervision of people engaged with secret documents and the cipher service. Their

technical training is the assignment of special organs of the NKVD. The technical part of this report will give details.

In various phases of the war the need became apparent of employing especially effective and dependable units at endangered points of the front or at strong points. For this recourse was had to NKVD troops and from these were formed the so called ОПЕРАТИВНЫЕ ВОЙСКА НКВД = operative troops NKVD, which were assigned in divisional units to the RKKA armies. The exact number of such elite divisions could not be established beyond all question by signal intelligence cryptanalytic means, but we can count on at least 20 divisions. It is significant that the principal use of these units was in the year 1942 and their employment decreased materially after the crisis was overcome. After the great turning point in the Russian theater, indeed from the moment when the Red Army shifted from defense to offense in almost all sectors and in a very short time showed good efficient units of the RKKA, the use of the operative troops NKVD ceased. It is not known whether the units were disbanded or assigned other tasks, possibly in the Far East, but in any case units of this kind did not appear after the middle of 1943.

Whereas after the beginning of the war the NKVD was able to handle the major portion of the resulting increase in work by the aid of the apparatus it had built up and developed in peacetime—sometimes with great expansion of personnel -- for combatting espionage, sabotage and the activity of enemy agents it became necessary to create a new organization which took over this activity formerly managed by the general organs of the NKVD.

This organization known as SMERSCH (СМЕРШ = СМЕРТЬ ШПИОНАМ = "death to spies") was formed from the section of the NKVD called NKGB (НКГБ = НАРОДНЫЙ КОММИССАРИАТ ГОСУДАРСТВЕННОЙ БЕЗОПАСНОСТИ = Peoples Commissariat for State security) which had likewise arisen during the war and was later transformed into an independent commissariat working in very close contact with NKVD. SMERSCH became sufficiently well known particularly in the final year [of the war] as respects its significance, method of functioning and employment, due to messages read. Units, groups, organs and individual functionaries of SMERSCH were assigned on a supplemental basis beginning about the middle of 1944 to all troop units of the RKKA and also to almost all NKVD units. The number of SMERSCH functionaries depended entirely on how big the unit, on the sector of the front where it was located, on whether in hostile territory or home territory, on the tasks assigned, on its reputation and on the amount of observed or suspected enemy agent activity in its area. Ostensibly SMERSCH, like the NKGB in general, was set up merely to combat enemy agents and espionage, practically it served not only this admitted purpose but was an additional guarantee of the Bolshevic conduct of the Russians themselves.

To the particular tasks of the NKVD in wartime belonged also the putting through of mobilization and the drafting of recruits for the RKKA, also the setting up of armies and units of foreign nationalities and their incorporation and employment within the framework of the RKKA was the duty of the NKVD organs, all the more since political considerations were here of decisive importance. The training and guidance of partisans, scouts, and agents behind the German front, which became

extremely important in the last two years of the war, was likewise the work of the NKVD.

We must not forget to mention that the NKVD offices and their organs — NKVD troops of various categories — performed their manifold and often not simple, though important tasks with astonishing rapidity and lack of compromise. To be sure, as a study of the messages showed this was done by applying to their own people methods which were not always humane and often were gruesome.

The difficulty of the service to be rendered by the organs of the NKVD is recognized by the special position its units occupied in the USSR. From deciphered messages dealing with this subject it could be proven that the pay of the NKVD units was essentially higher than that of the RKKA and the rations appear to have been better too.

As is clearly apparent, the NKVD and the newly created corresponding and coordinated NKGB combined all the functions and duties which were exercised for example in national socialist Germany by the secret military police, the Abwehr, the Gestapo, the SD and SS. So far as is known however no difficulties arose in Russia, as they did in Germany, in respect to competence because the covering organization, the leadership and administration of the NKVD in Moscow, alone was competent to deal with all differences of opinion which might arise. Beyond doubt the insight into the organizational structure of the NKVD made a deep impression in Germany and influenced in no unimportant way the working methods of the German organizations of that day.

The foregoing observations give a sketch of the structure and significance of the NKVD set-up as made possible by putting together results of years of work in signal intelligence. The third section of part 1 of this report gives examples of the type of messages which can be of great importance for the high command in spite of the brief period for which they are valid and which can, due to their multiplicity, give ultimately a well rounded picture if carefully evaluated.

Army and Air Force (RKKA)

1. Short Review of the development of the RKKA up to 1939.
2. Army and Air force during the occupation of Poland, Baltic lands, and parts of Romania.
3. Army and Air force during the Russo-Finnish war.
4. Army and Air force during the War 1941-1945.
   a. Before reorganization
   b. After reorganization.

Since in general a great deal has been written about the Red Army as such and its significance with respect to strength and effectiveness has been sufficiently demonstrated by the events of the war and since it is not the purpose of this report to enter into the subject in detail, the author will limit himself to a brief account such as could be had exclusively from deciphered messages of the years 1935-1945.

In the years down to 1937 the radio was little used by the actual army formations of the USSR while the already mentioned border troops belonging to the NKVD made abundant use of it in the years 1935—1936. Down to 1937 the army limited itself to the use of short term, simple systems, within a narrow frame work not extending beyond the military district, in many cases radiograms were sent only during maneuvers or in radio practice work. The air force down to this point used relatively simple little systems although for a relatively long time. In general little could be learned from the messages transmitted, generally they dealt with reports of starting and landing of individual machines, weather reports, [damage?] reports, status reports of air fields, machines and instruments and operational and traffic reports. Really only in the

days just before and after the first of May in the years 1936—1938 was traffic of Russian airforce stations and even ground-air traffic at all heavy. The grand parade on May 1 was seized upon by the airforce units as the occasion for radio practice on a large scale. With a brand new little code issued each year solely for this purpose all reports were transmitted regarding the meeting, arrivals and departures, events during flights such as emergency landings and damage reports, weather reports, etc. Since the number and type of the machines arriving from the different military districts were all recognized, this traffic was much more interesting and instructive than the messages sent during the remainder of the year.

But even in those years it could be determined with absolute certainty that the airforce was and remained an integral component of the RKKA and was not an independent part of the armed forces as it was in Germany, accordingly later on, after radio had become the general property of the Red Army, the more extensive cryptographic systems employed beyond the framework of the military districts were employed simultaneously and in common by army and airforce.

The top command organization of the Red Army was the General Staff in Moscow, subordinated to it in respect to the work and personnel were the command and administrative staffs of the individual military districts which were regularly stationed in the capitals of the states. These command staffs virtually never appeared on the air down to 1937, in general down to this point the RKKA appeared in the light of cryptanalysis as a purely experimental, though numerically vast undertaking.

Only with 1937 did the constitution and development of the Red Army begin to be reflected in the results of decipherment and evaluation but now it took on more and more concrete form from month to month, in large measure due to the rapid growth of traffic.

The following military districts became known from deciphered messages and were mentioned repeatedly.

МВО МОСКОВСКИЙ ВОЕННЫЕ ОКРУГ	= Military district Moskau
ЛВО ЛЕНИНГРАДСКИЙ " "	= Military district Leningrad
БВО БЕЛОРОССИЙСКИЙ " "	= Military district Weissrussland
УВО УКРАЙНСКИЙ " "	= Military District Ukraine
СКВО СЕВЕРКАВКАЗСКИЙ " "	= Military District Nordkaukasus
ЗАКВО ЗАКАВКАЗСКИЙ " "	= Military District Transkaukasus
ПРИВО ПРИВОЛЬСКИЙ " "	= Military district Volga
УРВО УРАЛЬСКИЙ " "	= Military district Ural
ДВО ДАЛЬНОВОСТОЧНЫЙ " "	= Military district Fern Ost

Military district Ukrain was divided later, about 1938, into the military districts:

КВО КИЕВСКИЙ ВОЕННЫЙ ОКРУГ	= Military District Kiew
ХВО ХАРЬКОВСКИЙ " "	= Military District Charkow

The largest unit of the army was the corps, it had three divisions, each with three regiments. The concept "army" did not appear until the beginning of the war. Especially noteworthy was the relatively high number of cavalry corps which later in the course of motorization where generally transformed into mixed corps. Armoured units also came into

being in the USSR during the war 1941--1945. In the years 1935--1938 hardly anything was recognized except infantry and cavalry corps and divisions, while so called "mot.mech" divisions (motorized-mechanized divisions), "mot" or simple "mech" divisions were mentioned in isolated cases during large scale maneuvers.

Nevertheless it can be stated that the total number of Soviet Ground Troops mentioned in publications available to the general public was probably never even approximately correct, the imperfect [cryptologic] observation of the RKKA exceeded the public figures by far.

Instead of the ranks usual in other countries, such as Lieutenant and General, the following designations were used in the RKKA:

КОМКОР Командир корпуса	Corps Commander	General
Командив " дивизии	Division Commander	Lieutenant General
Комбриг " бригады	Brigade Commander	Major General
Старший командир 1. ранга	Senior Commander of the first grade	Colonel
" " 2. "	Senior Commander 2nd grade	Lieutenant Colonel
" " 3. "	Senior Commander 3rd grade	Major
Средний " 1. "	Medium Commander first grade	Captain
" " 2. "	Medium Commander 2nd grade	1st Lieutenant
" " 3. "	Medium Commander 3rd grade	2nd Lieutenant

The non-commissioned officers, both top sergants and lower, were designated junior commanders.

The grades in the Russian army were and are the following:

All Generals are mentioned individually and by name.

СТАРШИЙ КОМАНДИРСКИЙ СОСТАВ	= senior commander corps	staff officers
СРЕДНИЙ " "	= medium commander corps	
МЛАДШИЙ " "	= junior commander corps	non-commissioned officers
РЯДОВОЙ СОСТАВ	= enlisted men (line)	

However as early as 1938 these "popular" designations which had been created during or shortly after the revolution gradually fell into disuse and the designations used in Russia before 1917 where again introduced. The grades remained unchanged.

The RKKA during the years 1935-1938 was constantly being expanded, one innovation followed on the heels of the other. The intensified motorization, which initially encountered great difficulties because technique and experience were lacking and highway conditions were catastrophic, at first led to compromise solutions. The quite inadequate system of maps, the antiquated maps scaled in versts and the use of maps produced in England with English measures, the current renaming of villages, towns and cities for "heroes of labor" or deserving revolutionists, the desire to accommodate the system to that of the adjacent countries—all these made necessary the printing of new maps in the kilometer system. Down to 1937—38 the Russians worked both with the old verst maps and with kilometer maps with English inscription, it is clear that this situation,

which made errors a matter of daily occurrence, was untenable in the long run. Supported by the effort to introduce the decimal system wherever possible, the hitherto customary names of weights were also discarded and gram and kilogram took their places.

What has been stated thus far might give the impression that the ground troops of the Red Army, which as has been said, were in a state of constant development and reorganization down to 1938, would not have been a factor to reckon with under any circumstances. To a limited degree that might have been true down to 1937 but it must be remembered that German observation by means of wireless was just in the development stage and was groping its way further eastward year after year. Even the military district of Moscow, after it became possible to observe it by monitoring, yielded a far different picture than the frontier districts Leningrad, White Russia and the Ukrain which had been monitored previously. Beyond a doubt the cadre troops of the Red Army, well trained units progressive in equipment could not be spotted in the three military districts mentioned but were present in great numbers in the military districts of Moscow, Volga and Ural. As will be seen in the technical part of this report it is significant that the first extensive cryptographic systems, which presupposed a rather high degree of training for their use, first appeared and were employed in these same military districts.

The airforce, down to 1938 an often disdained experiment of the Red Army as far as army men were concerned, still a mere infant, was now incorporated into the army as an active component. Here again difficulties had to be overcome, all the more since the types of planes used in those days met the demand made upon them only to a modest degree. For reconnaisance

purposes for instance only training planes were flown which were known by the designations -U1-,-U2-, and -U22-(УЧЕБНЫЙ САМОЛЕТ = training plane) and were generally old models.

The following types were flown in considerable numbers by the RKKA down to 1939

У1, 2. 22 = УЧЕБНЫЙ САМОЛЕТ = Training plane

ТБ 3 = ТЯЖЕЛЫЙ БОМБАРДИРОВЩИК = Heavy bomber

СБ = СКОРОСНОЙ БОМБАРДИРОВЩИК = Speedy bomber

АНТ = АНДРЕЙ НИКОЛАЕВИЧ ТУПЛЕВ = Multiple purpose plane (this last model followed closely the American Douglas type of those days).

Planes were combined into groups, these [were sub-divided] into three squadrons of two or three flights each. The number of planes within the groups varied, I recall that 27 planes constituted a pursuit group while a heavy bomber group had only 12 machines.

The airforce, although particularly in the war years essentially enlarged and improved, could not compete qualitatively with the ground forces, its successes, insofar as effectiveness can be compared, remained far behind those of the army.

When in 1939 the Russians occupied part of Poland in agreement with Germany, the impartial observer got a picture of a quite undisciplined inferior armed force. Apart from the fact that the troops themselves were hardly formed trained contingents, technical equipment was almost utterly lacking. It is remembered that in order to make an inspection trip, regimental commanders had to request an automobile from the division staff, it was also noted with merriment that the harness and reins of mounted units

and those of vehicles were made of rope and string and th t leather was almost entirely wanting. Since the invasion of the Russians could be observed in all phases by German Signal Intelligence, i. e.even defficiencies with respect to the training, discipline and equipment where made the basis for generalization, a completely distorted picture resulted and the actual striking power of the Soviet Union was misjudged. The lack of organization in planning the invasion went so far that Russian units repeatedly fired on one another, especially at night, where by the casualties did not stop with the wounded. Today it is generally known that the Cadre of the RKKA did not participate in Poland, the Baltic states or in the Russo-Finnish war and that this was intentionally a theatrical performance even at the cost of human lives as was shown later in the Finnish campaign. The occupation of Poland, Roumania and the Baltic States went off without friction. Although there was practically no resistance anywhere, plundering, oppression and acts of violance against the population where the order of the day. In radiograms lists of booty were constantly transmitted, among other things the simplest utensils such as writing utensils, kitchen and household equipment. However people were not arrested, dragged away and executed until the arrival of the NKVD troops who immediately covered the entire country with a net work of agents in order to nip in the bud any possible resistance movement. The airforce had no part in the actual occupation, there was no air reconnaisance, only after the occupation was completed were Soviet machines stationed on existing fields and a large number of new fields built.

In its first phases, after slight initial gains in territory on the coast of the Finnish gulf and on the Karelian Isthmus the Russo-Finnish war brought the Russians heavy reverses. Numerous regiments of poorly equipped, poorly trained troops, inexperienced in winter warfare, were almost entirely annihilated by the Finns, encircled divisions died of hunger and cold. The radio messages of encircled or cut off posts showed panicky mood in all cases. The situation changed little when General Stern, successor to General Blücher in the Far East, took over the supreme command. The Soviet air force due to the unfavorable weather and its then backward state made but feeble attacks and scarcely afforded any relief and support for the heavily engaged ground forces. Numerous emergency landings by Russian pilots on Finnish soil often gave the Fins undamaged machines which they then flew. It was all more astonishing therefore when after months of fighting, relatively small numbers of Cadre troops from the Military District of Moscow broke through the Mannerheim Line in the last brief phase of the war, motorized forces reached Helsingfors in a few hours and forced the capitulation of Finland in a few days.

At the beginning of the war 1941—1945 the battle-tried German troops were opposed in the border areas by relatively poorly trained units and by units recruited among the Lithuanians, Letts, and Estonians. Hence the great initial German successes must not be estimated too high. The same holds for the first meetings in the air. The Russians were flying completely antiquated machines, hopelessly inferior to those of the Germans, fighting in lines (Reihenflug) without persuit plane escort (Jägerbegleitung). However it is noteworthy that in contrast to the Russo-Finnish war a panicky

feeling was rarely observed after the expiration of six months and almost completely disappeared in the course of the first year.

It cannot be over emphasized that probably no foe learned more rapidly than the Russians. The reorganization of the RKKA after the first war winter or during the course of that winter is without parallel for speed and thoroughness. Aside from the reorganization in the cryptographic service (see technical part), there was probably no part of the armed forces, no unit however small, which was spared. In the first place all measures which up till then had given the war on the Russian side a Communist-International character were very cleverly changed. The Commissars, who up till then had to countersign every order of the commanders and exercised an often fateful influence on the morale of the troops, disappeared officially. Freedom of religion was proclaimed, the war was declared a campaign for the freeing of the Fatherland. Nevertheless an invisible political surveillance by the NKVD continued, unreliable commanders were transferred and thus disappeared more or less without attracting attention. The organization of the RKKA, both ground troops and air force, was altered. An army which down to March 1942 consisted of two to three corps, each with three divisions and 1—3 brigades, was now composed of 4 to 6 divisions while the number of brigades remained the same. The concept corps disappeared entirely for the moment and was then born only by cavalry and armoured units fighting outside the army as such. The consequence of this was that the number of armies increased materially since the personnel strength often merely corresponded to that of an overstrength corps of earlier days. Special units in great number were incorporated in the RKKA, armoured brigades and divisions, corps and armies modernized and

changed the appearance of the Soviet armed forces very materially. Especially hard hitting armies to close gaps in the front, to hold especially exposed positions or to reconquer lost positions were crated under the title УДАРНАЯАРМИЯ = striking army. The grouping of several grenade throwers mounted on trucks which came to be known as "Stalin-organ" began in 1941 and was soon employed on a large scale as a special arm.

The Russian designation of this arm and its translation is:
O.G.M.D. = О.Г.М. А. = ОСОБЫЙ ГРАНАТО-МИНОМЕТНЫЙ ДИВИЗИОН
= Special Grenade-mine-thrower section.

After Stalengrad, the great decisive turn in the war, the term "Guard", which at the time was one of the stated reasons for the revolution, was reintroduced and bestowed upon deserving units as a special distinction, furthermore troops which had been charged with regaining territory came to be known by the name of the region, city or river concerned, thus there are for example the divisions "Lemberg" "Warsaw", the regiments "Riga", "Koval", "Prut" and "Grodno".

The airforce which down to March 1942 was organized only in groups and squadrons was increased many fold in a few years, indeed in months; better types were produced or were finally put into use. There arose air regiments which were combined in the air army's long range fighter and long range bomber groups and new units of the ground organization like the RAB (РАБ) and BAO (БАО) = battlions of the ground personnel and the airfields guard. Even though the great bomber arm of the RKKA never flew missions comparable in numbers to those of its Western allies, it can

be said nevertheless that the increasing activity of the Russian airforce cover, especially as regards its low attack and fighter planes, bothered the German front line troops very much and in addition greatly disturbed and interferred with supply.

In connection with these startling innovations, improvements and changes in the structure of the red army I may once more call attention to the fact that the thesis loudly proclaimed by the German command in 1941/42, namely that the Red Army was about to collapse, -- a fateful error-- was a piece of utter nonsense. Exactly as at the time of the invasion of Poland and the Baltic provinces, during the first phases of the Finnish campaign and particularly after the supposedly irretrievable, catastrophic losses and defeats in the summer and autumn of 1941, the Russians pretended a weakness which induced their opponents to draw heavily on their reserve in order to speed up the apparently impending collapse of the RKKA.

On the basis of cautious estimates the Russians may have employed gradually somewhat more than 70 armies after the spring of 1942. If we figure an average per army of only 5 divisions and one independent brigade, the Russians had at least 350 divisions and 70 brigades in contact with the enemy during the course of 3 years. Independently of these there were committed the previously mentioned hard hitting armies [shock troops] some 10 in number, at least 25 armoured armies, independent cavalry and tank corps and combat units operating outside the army organization. From the evaluation of messages it could be established that actually there were armies from 1 to 70 or slightly above without break in numbering.

Of course they were not all in the front simultaneously but were often withdrawn in order to be brought back to strength, regrouped or even dissolved. After which they would reappear in other sectors at the front or vanish from the radio picture. If we consider that all these figures are too low rather than too high, if we add the contingents of the airforce, navy, NKVD troops and Partisans, then and only then can one get an idea of the numerical strength of the Russian armed forces.

It is simply inexplicable how the German command could ignore the current reports about the new formation of great units of the Red Army, including numerous armies, in rear areas while the battle of Stalingrad was on. These armies, as appeared later, were by no means composed of grey-beards and youngsters. But just as the German command rejected these disagreeable figures as untrue and the creation of a timid fancy, laughed at the number of new formations of air armies which were recognized by the cryptographic section, in the same way it was unwilling to believe in the increasing capacity of the industrial plants beyond the Urals, especially in the Kusnetzki Basin, where again the cryptographic section could repeatedly bring figures.

The Russian supreme command, the General Staff of the RKKA in Moscow, took into account in all military discussions the vast war industries beyond the Urals which were in those days as good as exempt from attack and whose capacity was virtually unknown abroad. The Red Army had as its allies Time, Winter and Space from the point of view of costing the enemy a maximum attrition of men and material, whereas it was able by drawing on its vast human reserve to throw against the enemy every new units recruited

from all areas of the huge country without committing the operational, very effective reserves held in the interior.

All these facts were known to the cryptographic section from intercepted material and often enough gave German Signal Intelligence reason to warn its own High Command but an often very short sighted attitude, and unwillingness to listen or to comprehend, and in the final years military and political impotence prevented effective counter measures. I shall only add that Signal Intelligence energetically opposed the conscious underestimation of the Soviet Army and Air Force and even before 1941 was able to present figures which in no wise corresponded to the assumptions desired by the High Command.

~~TOP SECRET~~

Intelligence results from the decipherment of messages of the Army, Air Force, NKVD and Partisan Radio.

1. Preface
2. Recognition of the enemy situation.
3. Recognition of operational and tactical measures.
   a. Concrete intention to attack and commit.
   b. Shifts of strength.
   c. Commitment of special troops.
   d. Bringing up of reserves.
4. Recognition of the supply situation.
5. Losses of men and materiel.
6. Replenishment of units and setting up of new ones.
7. State of health and morale of the troops.
8. Authenticators and recognition signs.
9. Situation in the rear areas.
10. Details regarding communication and transport situation.
11. Details regarding war production.
12. Partisan activity, scouts and employment of agents.
13. Polish resistance movement.
14. Signal Intelligence as a security coefficient of our own conduct of of the war and the most dependable source of information on objectives of attack and commitment.

The first two sections of part 1 gave a more or less rounded picture of the political and military structure of the Soviet Union as it could be drawn by Evaluation by collecting and piecing together deciphered radiograms during the course of the years. Before discussing the actual deciphered traffic, i. e. the single message and its diverse possible meanings, the following must be made clear:

Among the multitude of fully or partially deciphered messages by far the greatest part appears to the layman irrelevant, unimportant or outdated, but for the trained evaluator messages of this sort may sometimes be of decisive significance. The reason lies in the fact that frequently only the sum of unimportant messages of a network with slight hints such as family names, changes of wave length or call signs or data for traffic schedules, permit deductions which can only be made with the aid of the card file, memory, experience and actual dependable knowledge. Even with messages of older date additional information is gained of a tactical, if not of an operational value. As an example of this latter case it may be mentioned that an order to attack or to commit which is read late no longer gives our own command any opportunity for direct counter measures, yet the units which may be mentioned in the message signify a further supplement to the enemy situation, if they are not yet known.

Signal Intelligence in peacetime has the task of deciphering and making readable as many messages as possible, of developing the systems in use, of attracting a sufficiently large staff of collaborators and training them and then of working over the information gained from cryptanalytic activity. It must also see to it that the observation of networks and traffics hitherto unexplained is not broken off, i.e. that the treatment of unsolved cryptographic systems be guaranteed and everything tried in order to break them. Hence in peacetime it is chiefly a question of working for the distant future and of burying oneself in the subject as a science in order to be equal to the greatly increased demands in time of war. Of course cryptanalysis as a science must not go so far as to neglect the demands of

content evaluation and thus those of the General Staff, of the Political Leadership and the National Economy.

With the beginning of a war, Signal Intelligence is confronted by a new demand, fulfillment of which is only possible if adequate useful work has laid the foundation in peacetime. Now it is necessary to read actual messages to provide the operational commands with the basis for urgent measures. This is only possible if the messages are enciphered in systems which have already been broken or are far enough along in the breaking process so that fragments at least can be read. Of course with the Signal Intelligence which fulfills all these presuppositions there will be times when it will fall behind events -- for example when the enemy changes keys -- but the aim must always be to make these periods as few and far between and as short as possible.

The following discussions and reproductions of deciphered texts given from memory are adapted to the actual traffic of the war. They are intended to show to what a high degree signal intelligence was able to aid our own leaders in their decisions.

One of the most important tasks of signal intelligence is probably as exact, speedy and exhaustive a clarification of the enemy situation as possible, i. e. current determination of movements of all enemy units in and behind the front. Signal Intelligence performed this duty completely during the entire war, either through decipherment of enemy messages directly treating such movements or through evaluation of others which indirectly permitted recognition of the movements. Not infrequently it was possible to learn of impending changes from deciphered messages. The following typical

example of deciphered enemy messages will illustrate the types.

Direct evidence of movements:

Army message: To the Chief of Staff of the 287th Infantry Division.

Command Post of the 1032nd Infantry Regiment is located in the woods 2.5 km northeast of Ivanovo.

Regimental Commander Petrov.

Air Force Message: To the Commander of the 127th Air Pursuit Regiment. Send a Liason Officer to the Staff of the 4th Air Army at Poltava.

Signed Ssablin.

Indirect evidence of moments:

NKVD message: To the Chief of Staff.

On 12.8.44 at 0750 o'clock Red Army man Kosolov, Petr Wassiljevitch was arrested at the south exit of the village Dolgaya by a patrol of the 15th picket. He deserted the evening before from the 642nd Infantry Regiment of the 113th Infantry Division of the 16th Army. Leader of the picket Komarenko.

Army message: To the Chief of Staff of the 149th Infantry Division, copy to the Commanders of the 912th and 946th Infantry Regiments.

Enemy in strength of one regiment infantry and tanks had broken into our position. Enemy tank points are at northwest exit of the village Shirokaya and on the road Shirokaya-Tomakovka 3 km south of Shirokaya.
Request support.
Commander of the 933rd Infantry Regiment.

Impending change of position:

Army message: The radio station of the 267th Cavalry regiment is being dismantled. We are moving to Bolotye. End of traffic. You'll hear us again on 14.6 at 0600 o'clock.
Leader of the radio station.

~~TOP SECRET~~

NKVD message: To the Commander of the 96th NKVD regiment. Your left hand neighbor beginning 0090 o'clock on 16.4.44 is the 128th NKVD regiment. Establish contact. Chief of Staff of the NKVD front staff of the firstWhite Russian front. Colonel Lyssyj.

Even more important for our own operational leadership is the prompt recognition of enemy intention to attack and to commit since this gives a possibility of immediate counter measures. Signal intelligence is very often in a position to make deductions regarding enemy intentions not merely from various observed circumstances but through reading direct enemy orders for attack or commitment. While army orders for attack on a large scale (army) were regularly enciphered in the operational and tactical 5-digit cipher, the airforce sometimes used unimportant although not simple systems. Example of direct order for attack and for commitment.

Army Message: To the Commanders and Chiefs of Staff of the 172nd, 178th, 192nd and 193rd Infantry Divisions, the 73rd and 112th tank brigades.

Commander of the Army has ordered:

1. 172nd Infantry Division attacks on 14.6.43 at 0403 o'clock with the 460th Infantry Regiment in the direction of Gorovok with the objective of winning the south exit of Grodok by 1030 o'clock. Crossings over the river Klinka 3 and 5.5 km southwest of Gorodok are to be forced in conjunction with the 461st and 512th Infantry Regiment. Arrival of 112th Tank Brigade is to be awaited here.

2. 178th Infantry Division ..... (etc.),

3. .....

(similar orders to attack issued to the units enumerated in the address.)

4. .....Staff of the 27th Army 13.6.43

1730 o'clock map L: 100 000 Novogorje —

Chief of Staff of the Army Colonel Klin.

~~TOP SECRET~~

Air Force message: To the Commanders of the 65th and 79th Bomber Regiments and of the 134th Pursuit Regiment. In the night from the 25th to 26th of September enemy approaches in the area Jampol - Ternovka - Vishnopol and the assembly area in the woods 4km northwest of Novo Archangels are to be bombed. Report execution.
Chief of Staff of the 9th air army.

Prompt recognition of such concrete intentions of the enemy to attack often led to impressive German successes particularly in the first two years of the war. For instance in the early weeks of the war signal intelligence promptly recognized an order for large scale commitments of the Soviet bombers against the crossing of the Düna, this permitted taking counter measures which resulted in the destruction of more than 100 Soviet Bombers by German pursuit planes (Mölders) before they reached the target area. The great German victory in one of the convoy battles in the Arctic was likewise the result of a promptly deciphered radiogram reporting the situation, route, speed and size of the convoy.

Signal intelligence was always able to spot and report to the High Command preparations for large scale enemy operations, for example the formation of strong points. This information was not based on the content of individual messages but upon current observation of occurrences in the individual front sectors, whereby reports of shifts of strength were usually the decisive factor. Here increased importance attached not only to the analytic work but to operational and traffic evaluation since careful traffic analysis can note concentration of traffic even on nets whose positions have been located [DF] although nothing is known about them tactically or by cryptanalysis. Always informative and significant was the request for or the introduction of special units, generally of a type

indicating preparations for attack, e. g. O.G.M.D. (colloqually Stalin organ). Immediately pending operational plans were always associated with the appearance in the traffic of assult troops. The bringing up of reserves, which is often recognized by signal intelligence, did not necessarily point to impending attack but when other characteristic signs were present could very well signify wholesale preparations for major operations.

The following sample messages can lead one to expect operations if other signs are at hand.

Army message: To Rubin

Load by 18 April for 47 army 20 T-34 and 15 SIS.
Request escort troops of 1491st Infantry Regiment.
Maintain contact with us. Line test [?] follows.
Report execution.
Chief of Equipment and Supply of the Northwest front
Major Stepanov.

Army message: To the Chief of Staff of the 47th Army Colonel Petrushkin.
3 O.G.M.D. have arrived at the 273rd Infantry Division.

Only a limited amount of ammunition at hand.
Further supply and sharpshooters are expected.
Morale of the troops and condition of the vehicles good.
Chief of staff of the 273rd Infantry Division
Major Rylov.

Of only indirect, though in the long run not to be underestimated importance, was decipherment of supply messages from which a fairly clear picture of the enemy supply situation in the individual areas could be drawn. Knowledge of the supply situation, of available stocks of ammunition, of available motor fuel etc., sometimes permits accurate deductions as to the fighting strength particularly of encircled contingents. The author still recalls distinctly the current, almost uninterrupted information on the

supply situation of Soviet Troops in the Crimea during the late winter of 1942. At that time Signal Intelligence could report daily for almost every hostile unit the food supply and the stock of ammunition by caliber and number of shells, precise quantities of motor fuel and other stocks, sometimes the replenishment expected.

Example of ammunition report:

Army Message: To the Chief of Equipment of the Black Sea Army. Ammunition stocks of the 18 Black Sea Brigade: Mines (for mine throwers) 81 mm -- 470, 105 mm -- 62, PTO (ПТО=ПРОТИВО-ТАНКОВОЕ ОРУДИЕ = Anti-tank guns) 76mm -- 905, Rifle cartridges -- 18030.Romanov.

Of similar importance was the decipherment of enemy reports on his losses of personnal and materiel which at times could be deciphered currently along individual sectors. In the above mentioned phase in the Crimea Signal Intelligence was able to give specific reports almost daily. Such reports were generally a part of messages which also touched on other questions. The part coming into question would have approximately the following content:

Army message:.....4. Losses for the 23.2.42 of the 17th

Black Sea Brigade: killed-non-coms 3, enlisted men 11; wounded-officers 1, non-commissioned officers 2, enlisted men 24; missing-non-coms 1, enlisted men 17, killed-1 horse. Burned 2 T-34, hit 1. .....

Since such reports often ended with the present strength in personnel and materiel or were followed by such reports after a short time interval, they afforded a very useful picture. For instance the author recalls that the operational group "Popov" during its break through movement to the Sea

of Azov in the spring of 1943 reported in its daily reports the losses and also the strength with the greatest precision for each of its units. Since these messages were read the information could be utilized by the German command.

No less important for our own decision was knowledge of proposed or actually occurring replenishments of enemy units which could be gained from deciphered messages, often most precisely. The messages announcing the arrival of replacements usually contained illuminating details. Example of a report of a replacement transport.

Army message: ...send on the evening of 17.4.43 to Komarvka station 1 officer and 8 men to take charge of 740 replacements. Divide these as follows: Of the 172 tank men give 48 to the 36th guard tank brigade, 64 to the 174th tank brigade, the remaining 60 to the group Kustinov. Of the 43 radio men 21 to 174th tank brigade, the remaining 22 to the 216th motorized infantry brigade. Of the 64 MP men all to Kustinov. The remaining 461 men will be divided between your own and the 311th Infantry Division according to need. ....

Also the withdrawl of badly battered units from the front and their transfer to the interior for regrouping, as well as the setting up of entirely new units from the recruits, could often be recognized by Signal Intelligence. Thus it was possible to follow for a time during the winter of 1941/42 the setting up of two new armies, to learn various details regarding the training of the recruits and, most important of all, to recognize the probable date and area of commitment. Events later confirmed the essential accuracy of information gained from decipherment.

The picture of the fighting strength of the enemy was rounded out by decipherment of radiograms giving details as to the health and morale of

the troops. Reports of this character occurred especially frequently in the early months of the war and, coming mostly from units which had been cut off, often bore an alarming character. But even after the situation had stabilized the political leadership of the medium and small units sometimes had occasion to complain about sinking morale or open dissatisfaction. Noteworthy and significant for evaluation of the fighting spirit of the RKKA was the care observed during the entire war to suppress the obviously strong trend toward desertion in the ranks of the Red Army. An endeavor was made to counteract this by camouflaging the International Communist Bolshevist Ideal, which was not very dear to the heart of the fighting men of the RKKA, as a national patriotic affair. Signal Intelligence was able to observe the systematic arrangement to bring about such a change in the spirit of the troops.

Examples of messages dealing with morale, health, attempts at desertion and internal service.

Army message: To the Chief of Staff of the 33rd Army Colonel Rudin.

The morale of the troops is poor. Enemy pressure from the direction of Koslovo increases hourly. Attempts at desertion in the 113th armoured brigade are increasing, anti-tank ammunition is lacking. Please supply by air.
Chief of Staff Lieutenant Colon Burlayev.

Army message: To Lieutenant Burlayev.
The Commander of the 113th Armoured Brigade is to be relieved, he is to be brought to the front staff on 15 February. Provide sure escort.
Colonel Rudin, Kommissar Wernyj.

Army message: To the army staff.
The condition of health in the division is catastrophic.
Dysentary of epidemic proportions, 379 cases to date.
Request medical assistance.
Commander of 164th Infantry Division.

NKVD message: To the NKVD Front Staff of the 1st Ukranian Front.
It is reported that operative and mobile groups of the 128th NKVD regiment have repeatedly picked up and held Red Army men of various units of the 51st army who were encountered in the supply area without obvious reason. There is suspicion of desertion.
Commander of the 128th NKVD regiment.

Army message: To the Commanders of the Units of the 36th Infantry Division.

Give instructions regarding the latest speech of the Marshall of the Soviet Union, Comrad Joseph Stalin.
Chief of Staff of the 25th Army.

Sometimes decipherment of authenticators and pass words led to local, generally lesser successes. Such messages often gave the airplane markings for several days, occassionally for two or three weeks in advance, and their content was quite useful for our own command.

Example of a message regarding airplane markings:

Army and Air message: To the Commanders of the 105th, 67th, 264th, and 301st Infantry Divisions, 18th and 107th Armoured Brigades. For recognition of aircraft by army units signal—am a friendly plane — . On 23.5. by day dip the right wing twice, in the night from 23.5. to the 24.5. short flashes by plane lights for a period of 3 seconds. On 24.5. by day alternately dipping both wings 3 times, in the night from 24.5 to 25.5 2 white and 1 red rocket. On the .... etc.

Example of a message giving countersigns

NKVD message: Passwords for 27.11. Challenge "Taschkent", answer "Kasakstan". For the 28.11 challenge "Honor", answer "fame". For the ..... etc.

Primarily from the decipherment of radiograms of NKVD border and security troops employed in the security zone valuable deductions could be made as to the situation directly behind the Russian front. From this traffic it could be seen that the difficulties caused by German agents dropped at night behind the Soviet line were considerable and called for extensive action in defense. Knowledge of the measures taken by the Soviets again and again made it possible to perfect our method of employing agents. Bands operating in the Soviet supply area, anti-Soviet Ukranian and Baltic elements and small groups of deserters from the RKKA, caused considerable disruptions. Knowledge of the existence and activity of such "indirect allies" gave the German leaders a chance to incorporate them in their plans and led to support of such groups with materiel. The extent of these disturbances becomes evident from the fact that the NKVD Security Troops were often obliged to employ rather considerable contingents -- sometimes several regiments and even operative NKVD divisions -- to liquidate these bands. Thus the 18th NKVD Cavalry Regiment was tied up in the southern Unraine over 4 weeks by one such action.

Examples of messages of Border and Security Troops NKVD showing assignments in the supply area of the front.

NKVD message: To the commanders of NKVD regiments 103,86,and 87.

The forest area coordinates 4721,4719,4720,4819, 4820 and 4821 is to be combed thoroughly, dispersed enemy groups are to be liquidated, the formation of bands with the aid of the populace is to be prevented under all circumstances. Report whether it is wise to evacuate or to shift population. See to putting the roads in repair. Report execution at once.

Chief of the NKVD Front Staff of the second Ukranian front Colonel Kusnetzov.

NKVD message: To outposts 4,6,7,8 and 9. In the night from 4th to 5th October the enemy dropped agents in the area 6211, 6212, 6311.
Take measures to find them.
Commander of the 68th NKVD regiment.

NIVD message: To the Commander of the 68th NKVD Regiment.
On 8 October
civilian Pavel, Ivanovitsh Jershov, was arrested, 25 years old, dark blond hair, blue eyes, medium height -- stocky, no special marks of identification, dressed in a green jacket, old grey trousers (Stiefelhosen) and black army boots, without proper papers.
Leader of the 8th outpost Lieutenant Bogdanov.

NIVD message: To the Commander of the 74th NKVD regiment.
The villages Sloveni and Krassilovo are to be de-populated. Use all inhabitants capable of labor for bringing up motor fuel [?] on the auto road [?] between Sloveni and Tolotshin, for the rest proceed according to normal instructions.

Chief of Staff NKVD of the Second Ukrain front--Colonel Pushkin.

To the reconnaisance of the situation in the rear area belongs the recognition by signal intelligence of traffic conditions on Soviet railways, waterways and highways. Reports read showing overburdening of particular stretches, the assembling of transports at particular points, the re-routing of certain supplies, not only provided useful hints for the employment of

of armament plants beyond the Urals.

With the coming of winter 1942 partisan activity began in the White Russian territory occupied by Germany and in the course of time this spread over practically the entire German supply area. These units operating on very different scales were at first entirely on their own but later were combined into a general partisan organization and their employment was regulated from the Soviet Union. Special staffs of the partisan movement were created which cooperated with the front staffs of the NKVD troops in the particular region. Determining the location of such partisan groups and combatting them was possible only by watching the radio traffic between the groups and their staffs and deciphering the messages.

Like organs for partisan control guided the employment of groups of scouts and agents in the German rear, even in Germany itself; these agents were generally dropped from planes. Here again it was up to Signal Intelligence to make it possible to find these agents. However although a large portion of army, navy and NKVD systems were read, taking them on a percentage basis, decipherment of partisan, scout and agent messages was far more difficult, in part impossible. This was due to the great number of different systems — actually each agent had his own keys, to the difficulty of the ciphers themselves — individual additive systems, double transpositions, and grilles — but even more to the scant amount of homogeneous material.

Examples of Partisan, Scout and Agent messages.

Small transports of troops on the auto road.

Little rail traffic, principally wounded from the front.

Burlak.

To Group Rodina

Prevent bringing up supplies on the stretch Ossipovitshi—Bobruisk by blowing up the temporary bridge over the Volanka.

Staff Ssablya.

To Staff Pusa:

The agents Feodr, Abramovitsch Listov — Bobruisk, Gorki St. 14 and Ivan Gavrilovitch Rudenko—Bobruisk, street of the October Revolution 1927 are to be shadowed. They are suspected of communicating with the enemy.

Nikitin.

Our station recognized, moving to 3rd alternate position.

Request new key material, food and money via Mitia.

Calling again at 2300 o'clock.

Goldmann.

Toward the last, 1944/45, reports of this kind had to be taken very seriously for they showed indirectly the conditions behind the German front and in the often insecure supply area. In many cases it was possible through reading such messages to prevent single acts of sabotage and partisan attacks or to pick up agents or scouts. However the great lack of personnel on the eastern front was decisive in this matter, the security units of the German Armed Forces consisting of "old gentlemen" were hardly ever able to achieve important successes in combatting these organizations on the basis of perfectly good hints from Signal Intelligence.

In the final phase of the war abundant traffic could be intercepted

which when deciphered revealed the activity of a Polish nationalist movement. From the content it could be learned that this movement for the moment adopted a waiting attitude with regard to the Soviet Union and received its directives directly from London. It could be recognized that this organization then in the course of formation was pursued by NKVD organs as became evident from numerous reports about arrests of their members by the Russians. There were also repeated complaints of acts of terrorism in the part of the NKVD. The texts of these messages were in the Polish language and were concerned with the need for setting up, expanding and strengthening the organization. The scanty deliveries of arms, inadequate propaganda material, an unreliable and war weary attitude on the part of the Polish population prevented this nationalist movement from becoming an important factor. Absolutely anti-German in the beginning, rather pro-Russian, as a result of the brutal acts of the Russians and the constant arrests of its leaders, the movement became definitely hostile to the Soviets and for a time was inclined to make common cause with German minorities and isolated Baltic groups. The NKVD units knew how to reduce this party very quickly to the status of an insignificant underground movement by using its own agents and denunciations, by arrest, sending into exile and execution.

The examples given probably show quite clearly the importance of a Signal Intelligence Organization. Carried on systematically and continuously it affords in peacetime quite important information regarding the development of various branches in the country under observation. Often it permits deductions as to the true intentions which the country under observation may

be striving more or less cleverly to conceal. In time of war the value of Signal Intelligence is obvious. It warns its own command by giving it enemy plans, it enables the command to make its disposition with reasonable security, by sketching the situation and strength of the enemy, and it points out weak enemy positions and profitable targets for attack. Thus to a certain extent Signal Intelligence eliminates the uncertainty and therefore the risk from military actions. It is perhaps the youngest branch of the service but already has considerable acumen and when employed intelligently and on a large scale must not be underestimated either in defensive or offensive warfare.

Part II Technical Part

After giving in Part I an overall picture of the Soviet Army and Airforce and of the political organization of the NKVD and having shown the individual cipher messages without any technical commentary, these messages which are the stones of which Evaluation constructs its mosaic, we will now discuss Russian cryptography and give details of the individual systems.

Since a description of this material presupposes a certain acquaintance with technical expressions, an alphabetic compilation of these terms with brief explanations has been included in Part IV (appendices). The appendices include also illustrations, sketches, and tables on single sheets which make it possible to compare the descriptions in the text with such presentation. All drawings, plans, sketches and tables are schematic reproductions, since without exception they had to be made up from memory. In general they are close to the real article and in handling and structure should coincide completely with the real thing. The figures in the survey of performance and status are roughly rounded out and are consciously taken too low rather than too high.

It need only be added that in this technical part the author fully guarantees the essentially accuracy of this statement, both in respect to the text and to the graphic reproduction.

Russian cryptography

In structure and organization.

I. Army and airforce.

a. The 8th Section of the General Staff of the RKKA and its subordinate organs.

b. Basic changes during the war down to the status of the spring 1945.

2. NKVD

a. Direction and control of the NKVD cryptographic work.

b. Brief survey of internal traffic.

c. Traffic of Partisans, Scouts, and Agents.

The chapter on Russian cryptography in structure and organization is the only section of this report not derived exclusively from results of decipherment. It must be evident that the structure of the 8th Section of the General Staff in Moscow and its functions could not be the subject of enciphered communications but that knowledge regarding it must be secured from other sources. For this reason all prisoners and deserters suspected of having even the slightest official connection with these matters were turned over for interrogation to the control station of Signal Intelligence. In most cases the author conducted the interrogations himself and thanks to these and to information obtained by decipherment and capture he was able to draw a practically complete picture of the structure of this control organization which corresponded very closely to the facts. The reasons which early in 1942 forced the Russians to depart from their previous habits in cryptographic matters are proven by events as these statements will show.

The highest authority and hence the controlling office for all matters connected with cryptography in the army and air force of the Soviet Union is the 8th Section of the General Staff of the RKKA in Moscow. Directly subordinated to it are all 8th Sections of the staffs of the front, of armies, and corps and all 6th Sections of divisions and brigades as well as the SCHO (SHO) = ШО=ШИФР. ОТДЕЛ. = cipher sections of the lower echelons. The 8th Section of the General Staff in Moscow is subdivided according to its duties into three groups, of which each takes over a number of functions. Constitution of the 8th Section of the General Staff of the RKKA.

Group 1: Personnel matters.

Issue and recall of cryptographic materials for the army and airforce.

Production of cryptographic materials.

Registering all cipher messages in operational and tactical systems.

Group 2: Working out of mechanical aids.

Development of cryptographic materials and checking proposals relating thereto.

Group 3: Employment of РАДИОРАЗВЕДКА =

radio reconnaisance.

Cryptanalysis

Evaluation.

The first group also is, for all practical purposes, the administration of the 8th Section, in close contact with the NKVD it is responsible for selection and maintenance of cryptographic personnel, it sets up training

courses and distributes the trained men according to needs. Up to the spring of 1942 Group 1 was solely responsible for the distribution of cryptographic materials but was obliged to give up this function, as events showed. However it remained responsible for the issue, recall and replacement of the operational-tactical 5-digit system (Chiffre) and had to provide current means of encipherment (additive sequence) for this cryptographic system. All radio messages in this most important Russian system were sent in the original, after they had fulfilled their immediate purpose, to Group 1 of the 8th Section and were here sorted and filed from the point of view of military history. They were intended to form the basis for a subsequent general staff study as was repeatedly stated by captured higher officers.

The task of working out new cryptographic material was divided between the first and second group. While the second group undertook the purely theoretical development according to cryptologic principals, the first group checked these with respect to suitability and convenience. Among the duties of Group 2 belong the compilation of the 5-place, virtually endless digit-sequences (additive sequence) used for enciphering the operational-tactical Chiffre. Systems of call signs and wave allocations were also worked out here. Beyond that, Group 2 was occupied checking proposals received from people outside. After the shift in 1942 Group 2 devoted its principal attention to the development of Baudot traffic.

Group 3 had essentially the same tasks as Signal Intelligence in the German army. However, while the importance of this intelligence agency could no longer be questioned in Germany, due to its successes, the third

group of the 8th Section of the General Staff in Moscow may have remained a stepchild down to the final years of the war.

In the choice of Signals personnel, in particular of those working with cipher, an extraordinarily strict rule was applied down to the beginning of 1942. It is known from repeated interrogations and confirmed by captured material that all members of the 8th Section or its subordinate organs, hence down to the last SCHO member in the smallest unit, had to be old party members and absolutely reliable in their political views. Hence selection of this personnel was made under absolute control of the NKVD. Moreover the two special schools for cipher personnel in Moscow and Tambov were conducted by the NKVD. Before the war and down to early 1942 the period of training at these schools was 6 months. Aside from operating very varied ciphers, the history of cryptography was taught in condensed form and the field of cryptanalysis was touched upon briefly. However, it is certain that no decipherment of any type of foreign cryptograms was taught and practiced at these schools and that the brief glimpse of cryptanalysis was only intended to demonstrate to the pupils that such a thing existed and to train and inspire them to precise, responsible use of cryptographic material. Thus one prisoner, a Russian captain in the cryptographic field, stated in the course of the interrogation that at both the schools for cipher personnel great attention was paid to the time of the World War 1914/18 in the history lessons on cryptography. The significance of cryptograms as such is emphasized by historic events which can influence the course of operations, e.g. the prelude to the battle of Tannenberg where the Russians sent their messages in clear because both partners had different cryptographic material. After the heavy losses in the summer and autumn of 1941, also among crypto-

graphic personnel, it was necessary to change the requirements regarding selection and to reduce the training period at the schools. The Russian with his ingrained tendency to allow only the smallest possible number of people any insight into secret matters had not been able to make provision for the loss of trained people and provide trained replacements at once, he was therefore obliged to give up an all too strict and thorough selection of cryptographic personnel. Since 1943 especially suitable non-members of the communist party can be employed as cryptographers, if they are otherwise dependable, the period of training which was first reduced to three months has since 1943 been only one month. Due to the high personnel losses the numbers in the 8th and 6th Sections respectively had to be sharply reduced and the great loss of officers now led to the introduction of civilian officials as directors of 6th and 8th Sections of the corps. As I remember, personnel strength of these sections, before and after the reduction, was stated by prisoners as follows:

	Before the Reduction	After the reduction
Front Staff (8th Section)	Chief;Lt.Colonel 2 officers; 20 men	Chief; Major 1 officer; 15 men
Army Staff (8th Section)	Chief; Major 2 officers;12—15 men	Chief; Captain 1 officer; 10 men
Corps staff (8th Section)	Chief; Captain 1 officer; 10 men	Chief; Adjutant (1st Regiment), 6 men
Divisional staff (6th Section)	Chief; 1st Lt. 6 men	Chief; Adjutant 2nd Regiment 3 men
Brigade Staff (6th Section)	Similar to division staff.	

Interesting and illuminating for the importance of secrecy is the fact that the sections working with ciphers at the individual Staff could only be entered by the Commander, his deputy and the highest political functionary and that, aside from the Section Chief of the moment, only these had the right to check the work of the individual cipher clerks. The cipher personnel on its part was only permitted to take orders from its immediate superior, i. e. the chief of the Section concerned. Since the chief of the cipher section, at least in the first year, was an old party member and thus very often closer to the political functionary of the unit than to the Commander, there were often disagreeable conflicts which might ultimately lead to an absolute split between political and military leadership. In any case down to the middle of 1942 it was practically impossible for the Commander to send a report by radio without the knowledge and counter signature of the Commissar whether to a superior office or only to subordinate formations. This untenable situation came to an end with the basic changes in the course of 1942, the competences of the political leadership were clipped pro forma in harmony with the proclamation of the war as a fatherland crusade and the Commanders now obtained the right to make their decisions themselves. Practically however everything remained the same since the Commissar still had the right to read all messages and could, if he choose, use these as proof against the military leadership.

Since cuts in personnel and training time doubtless occurred in other parts of the Signal Service at the same time, it was comprehensible that performance and dependability of the operators and cipher clerks must suffer thereby and consequently more errors appeared in cipher messages which frequently made decipherment much more difficult. Frequent inquiries on

many Russian circuits and requests for repetition or changes of key proved that the consequences of the cut and the difficulties in their own operations were becoming noticeable. These facts were doubtless one of the reasons for the rapid extension of Baudot lines in internal communications, in this way it was possible to spare communications personnel in the interior. Whether in addition to Baudot, cipher teleprinters and more recently speech scrambling machines, pure cipher machines have also came into use on internal circuits is not quite certain, however it can be stated that traffic in machine systems had not appeared on military circuits up to May 1945. One cannot escape the impression that the Russians prefer manual encipherment, at least for use with the armed forces, all the more since in the use of 1-time additive he has found the ideal system of encipherment.

According to the statements of prisoners, deserters and agents, Russian radio intelligence attaches primary importance to traffic analysis, direction finding and observation of operations while ostensibly cryptanalysis was able to show only scant results in spite of extensive employment of the 8th Section in Moscow. This statement is based solely on such testimony and cannot be proven since there is no possibility of checking on it. On the other hand it is certain that a large staff of scientific employees, including linguists and mathematicians, was active in cryptanalytic work in the 8th Section of the General Staff in Moscow and it is quite possible that more or less success was achieved in this field if we consider the Russian mentality, their aptness and talent for mathematical matters and secret affairs. We may add that among the "temporarily secret"

ciphers and emergency keys used by the Germans were some systems which were anything but secure and that in the beginning armored units for instance used Signal Codes whose composition and encipherment would not even be considered today. Russian traffic analysis was able during the war to achieve very considerable successes to the sorrow of the German command by intensive use of men and equipment and uninterrupted observation of various German circuits. Thus for instance the Russians monitored with great persistence the arrival and departure of German planes at all sorts of airfields. An antiquated system of call signs on the German part often gave them a chance to determine the number of planes and their type and to recognize what they were doing. Far more unpleasant for the German front in the East, which was often very thinly held in insufficient depth, was the fact that the Russians by studying indicator groups and by direction finding recognized the joints in the German front and concentrated their attacks on these points which, as everyone knows, are likely to be the weakest. Cryptanalysis in the army at the front accounted for only a little developed, quite unessential part of the Russian Signal troops, a few front Staffs had units for cryptanalytic work but from the army down to the division only a few intercept operators and DF men were available.

Preparation and issue of new cryptographic systems as well as withdrawal of those to be replaced was exclusively the duty of the 8th Section of the General Staff in Moscow till March 1942. In this way a unified direction and control was possible and the issue of only a few general systems had the advantage that these were well mastered by the cryptographic personnel and that errors in general could be avoided. It is obvious that this type of

unified direction was also of great advantage for unauthorized decipherment because a concentration of homogeneous traffic made possible a break into the enemy systems and the relatively long period of use of the single system as well as the very limited number was what made possible expanding these breaks. After the first few months of the war between Germany and the Soviet Union the necessity became apparent of making basic changes in respect to the composition and distribution of cryptographic systems.

The rapid German advance during the summer and autumn of 1941 inevitably resulted in the German capture of numerous Soviet cryptographic documents of the army and airforce. Since when they were used universally the capture of a single copy was sufficient to expose the systems of the entire front, it was obvious that the Soviet Supreme Command had to make a change as quickly as possible. This basic change in the organization of its cryptography in a period which was exceedingly critical for the USSR was put through in the notably brief period of three months, using threats of the severest penalties for any delays or contraventions, and by the expiration of the month of March 1942 was everywhere completed. In contrast to the centralization of peacetimes the construction and distribution of cipher material was now decentralized. Only the preparation and issue of the operational and tactical 5-digit code (Chiffre) was still reserved for the 8th Section of the General Staff in Moscow while the front systems—called from now on SUV = СУВ = СКРЫТОЕ УПРАВЛЕНИЕ ВОЙСК = camouflaged communications of the Command, were worked out by the Signal Chiefs of the subordinate units, issued at their discretion and replaced when there was danger of capture. The systems thus originated were distributed to the subordinate units and to the nighbor to the right. For the

setting up and working out of SUV systems by the individual Signal Chiefs a scheme was worked out by the 8th Section in Moscow which outlined in a general way the size and character of such ciphers but contained no directives as to the choice of encipherment. The 4-digit codes with 3000 to 10,000 groups, which had been used in common by the army and the airforce down to the beginning of 1942, for army — corps — division — brigade — regiment, were withdrawn, although according to their own statements codes of this type had appeared absolutely secure down to 1942, inasmuch as the encipherment tables were different from all larger formations. One code of this kind, the "OKK-5", was captured by the Finns during the Russo-Finnish war and a copy was passed on to the German High Command. Although, according to a radiogram, the loss of this code was known to the Russians, only the compromised encipherment table was withdrawn while the system as such remained in use for months. It may be assured that only the very frequent capture of such systems with the most varied encipherment tables finally induced the Russians not to use systems of this kind in the army and air-force for the time being. Although according to the statements of prisoners other large 4-place codes were in preparation, none of them appeared again down to the date of capitulation.

It is solely due to this change in cryptographic organization that the readability, especially of army messages, became less and the capture of new systems, which were employed in a small area, no longer endangered the whole. The multiplicity of such systems, the relatively slight amount of intercepted traffic on the individual nets and the brief period of validity — particularly in the army, made decipherment extremely difficult and often made work on small and very small groups of messages an impossibility. If in

spite of this it was possible right down to the final days of the war to provide the high command with important reports, often when our own communications system was having great trouble, this was exclusively due to the fact that the former German army had plenty of trained, practiced cryptanalytic personnel. Compare appendix 3, part IV — Chart of general types of cryptographic systems arranged by size and area of use.

At the end of the section dealing with cryptographic systems of the army and airforce the surmise may be ventured that the 8th Section of the General Staff in Moscow may, now that the war is over, return to the former centralization of compilation and issue of cryptographic material. The author sees reasons for this in the fact that 1) administration and control of the elaborate set-up can be handled much more easily in this way and 2) in the reflection that the sole cause for the change in 1942 — the possibility of capture by the enemy of secret documents — no longer holds. This change would be very important for our own cryptanalysis since, assuming a long period of use and resultant greater mass of intercepts within any given system, it would allow devoting much care to work on the systems and result in the reading of completely deciphered messages rather than mere fragments. The only question is, how far the Russian may have been induced by the experience of the war, in particular by inspection of the results of German cryptanalysis and the statements of prisoners, to change his cryptographic system and radio communications further in any basic way and to adapt them to present day requirements. The answer to this question can only be given by sifting and studying actual message material.

Central Office for the cryptographic office of the NKVD organ is located with the GUP-NKVD in Moscow. Organization and function of this

Section in the field of NKVD cryptography are not known. In contrast to the cryptographic systems of the army and the airforce it was never possible to capture NKVD systems which were in use. At various points in the front 4-place NKVD codes did fall into the hands of German troops but these were already out of use or were reserve systems which because of the compromise never were put into use. Consequently the NKVD Cryptographic Central Office in Moscow was able to maintain throughout the entire war its method of centralization for the preparation, issue and recall of cryptographic material. For this reason the Section of GUR-NKVD corresponding to the 8th Section of the General Staff of the RHKA was not obliged to make any radical change in the further developments of cryptographic systems as such but remained substantially unchanged from the time we began systematic observation down to the day of capitulation. Therefore in spite of the great number of different NKVD organs there was only a limited number of NKVD cipher systems in use and these remained in use for a relatively long time, often more than two years. This gave the chance for our cryptanalysts to do extensive work and led eventually to what often was 100% readability. However one must not make the mistake of regarding the NKVD systems as simple, easily broken ones, on the contrary from the beginning they resisted systematic analysis extremely well and the ultimate complete readibility was only due to the long period of use and the consequent great amounts of homogeneous material and to the untiring industry of those who worked on them. It sounds paradoxical to say that the cipher section regarded every relatively important capture of cryptographic material with very mixed feelings. Even though captured material frequently made possible complete working out of partially broken systems, on the other hand the inevitable

consequence was the replacement of these systems which were now completely legible but soon out of use. Since as already mentioned live NKVD material never fell into German hands, it was possible in the cipher section to accomplish more with far less personnel with NKVD then with army and airforce systems.

The monitoring and deciphering of internal radio traffic was not an assignment of army signal intelligence units but necessarily messages of internal networks were solved and worked on. Special offices in the former German army were occupied among other things with the reception of messages of Baudot circuits, the value of the results however belonged in a different sector. Even in the years 1938/39 a relatively simple device was constructed which made it possible to reproduce directly on typewriters the Baudot messages which in part were transmitted by high-speed transmitters. The results from the point of view of content in no wise corresponded to the expectations. Of the entire traffic monitored at great expense at best 10% was useful for economic leaders while military-political matters constituted hardly 1%. The major portion of these messages was like the content of the long distance telephone messages and contained private or business affairs. It was learned that all these circuits were not only monitored and controlled by the NKVD but in many cases were directed by it, and that in all probability the GUP - NKVD was also responsible in large measure for the issue of cryptographic material for internal radio traffic.

The NKVD also had an important share in preparation and issue of cryptographic material for partisans, scouts, and agents. With the original multitude of partisans operating independently and with the mass employment of agents and scouts in the enemy's rear, provision had to be made for

current replacement of cryptographic material whereby it was of prime importance that the systems be handy, simple to use and yet secure. This task could not be accomplished by a single central office however big, hence the individual partisan staffs, which were generally in the immediate vacinity of army and also NKVD front staffs, were assigned production and distribution units for such cryptographic systems although all such units were under the guidance and control of the NKVD. Although the systems used in partisan, scout, and agent traffic, from the simplest to the most difficult, included some which were neither theoretically or practically capable of solution, it can be stated with good reason that in many respects much latitude was afforded the individual imagination and discretion. A norm, similar to that in the SUV systems of the army and airforce, did not exist, the structure and use of cryptographic means had to be adapted here to the momentary needs of agents who often worked alone.

From the foregoing it again is apparent to what an extent the NKVD exerted an influence in affairs of the army and airforce and also in the economic field. Since 1944 the NKGB has gained increasing influence in the economic field and taken over some function, especially those of control, from the NKVD. This does not by any means indicate the weakening of the NKVD but is based solely on an overburdening of the latter with too many other assignments. Although many people may entertain the opinion that the NKVD in consequence of its employment and influence in all fields and of the vast number of people engaged and its long period of existance is suffering from over-organization, it can be asserted on the other hand that this organization had a very important part in getting through the crises and

in the victory of the Soviet Union over the German armed forces. Especially noteworthy is the high degree of education and responsibility of the NKVD personnel which during the entire war prevented any NKVD cryptographic materials in current use from falling into the hands of the enemy.

The development of Russian Military and Political cryptographic systems in the light of cryptanalysis.

1. Systems of army, airforce and NKVD

   a. Operational systems
   b. Signaltafeln [very small codes]
   c. Address codes
   d. Substitution systems.
   e. Transposition systems
   f. Additive systems.

2. Systems of Partisans, Scouts, and Agents.

3. Encipherment and Disguise of Coordinates.

The relatively advanced state of decipherment of Russian material in the former German army was due primarily to the fact that systematic observation of Russian military and political radio traffic and also work on the messages, i. e. decipherment, was begun early. The development of Russian cryptography shows how important it is to start decipherment of the cryptograms of a country whenever possible at a point where the cryptography of the country in question is still primitive. It is then necessary under all circumstances to continue observation of the traffic without breaks even for a brief period since otherwise ones own signal intelligence finds it difficult or even impossible to keep step with developments. In the case of Russia it was possible for the former German signal intelligence to meet all requirements for a favorable development of Russian decryption, as the following historical cryptographic review will prove.

At the outset we may mention the fact that no recipe can be given for cryptanalysis itself, i. e. for the general ability to break unknown

systems and reduce them to a readable state. The ability to decipher will always depend upon a certain gift and upon good general knowledge, linguists and mathematicians being equally important. Naturally the analyst uses much traditional knowledge such as frequencies of letters, bigrams, trigrams, syllables and words while mathematical fundamentals of combinatory analysis, theory of series and theory of probability find application, however knowledge acquired in all these can never replace the knack of a good cryptanalyst. In the course of time it was possible to develop in various fields of cryptanalysis noteworthy aids in the handling of unknown traffic, to work out methods and build mechanical gadgets which are able to speed up and facilitate decipherment. Precise, penetrating linguistic studies contributed their share to facilitating and simplifying the analyst's task. However within the frame work of this report it is not possible to go into details respecting such aids and methods and a discussion of these must be left for a possible further report. The same holds true regarding the training of replacements for signal intelligence in general and for a Russian staff in particular. The selection of personnel should be made with due regard for what practice and theory have taught, which points will be touched on briefly in the first part of the report.

For various reasons, but primarily to avoid a confusion of technical expressions and concepts, the various types of systems will be treated in what follows irrespective of whether they were used by army and airforce or by the NKVD.

The development of Russian cryptography in general and the perfecting, expanding and the increasing of type complexity of the several systems are

a reflection of the development of the RKKA itself. Even though the cryptographic systems of the years 1935--1937 were in the main simple and very simple ciphers which scarcely merit the name cryptographic systems today, it is necessary to discuss them if we are to show the development of Russian cryptography. Primarily these early systems were so called operational systems, simple to use-whether for encipherment or decipherment, and serving in the beginning almost exclusively for operational needs. Almost the entire radio traffic of the army and airforce in 1935/36 served primarily for instructing the personnel in the secrets of all matters connected with radio.

All cryptograms intended primarily for operational-technical messages fall under the heading "operational systems". As examples a few messages may be reproduced.

> Our station will operate tomorrow from 0700 -- 1100 o'clock and from 1500 to 1900 o'clock. Lewtschenko.
>
> Why do you not answer all calls?
> Our wave length is 157.
>
> To the head of the radio station.
> Your operators are performing badly. Have them relieved.
> Chief--Signal Officer.

It should be clear that messages of this type were almost absolutely worthless for evaluation of content and that they could be used solely for operational studies. Nevertheless this material was important even for German Signal Intelligence in order to get accustomed to Russian traffic since in this way one could become acquainted with the habits, peculiarities and manner of sending, message structure and use of call signs and wave lengths and, as already mentioned, was able to keep step with the observed situation. Later on even operational traffic sometimes gained in significance

when such a cipher was used as emergency system by encircled units as was the case during the years 1941/45.

All these systems, almost entirely substitutions and in rare cases small codes, are termed PT = ПТ = ПЕРГОРНАЯ ТАБЛИЦА = chatter tables. The first operational system employed for a long time by the army and airforce of the entire Soviet Union was the PT—35 (chatter table of the year 1935). This table did not appear in traffic until late 1936, it contained 100 groups and had a new encipherment almost every day within the individual network.

Compare Appendices 4 and 4a.

The 10x10 number squares serving as keys were called "system squares" and rendered our cryptanalysis and especially our operational and traffic evaluation very valuable service in respect to identification of circuits since the call signs of the different stations were taken from the same square with the same numerical orientations as the cipher elements used to encipher texts. In general three to four system squares were used alternately in one military district and these remained in service up to two years. Consequently it was quite possible — and was repeatedly established-that keys which had once occurred were used again after not too long a time. At times an indicator was prefixed to the enciphered text consisting of two digits of which the ten indicated the first and the unit the second key sequence of the system square used for encipherment.

In the final months of 1939 the PT-35 was replaced by the PT-39. In contrast to the one it replaced this operational table showed some variants

and contained two switch groups indicating how these were to be read. These switch groups, each having one group in the code, served to tell the cipher clerk which of two possible meanings of a group to choose. Appropriately enough these switch groups read:

1. Read letters (single letters),
2. Read words.

The type of encipherment with the PT 39 was essentially the same as with the PT—35, the system squares were changed somewhat more frequently.

Compare Appendices 5 and 5a.

Early in 1942 the PT 41 succeeded the PT-39. It was of the same size (10x10), 98 cells out of the hundred had two meanings, again two switch groups indicate which meaning is to be taken. The alphabet and the digits 0—9 always had two values, the most common letters:

O, И, E, H, T, A, B, C, P, K, and a few others had 3 values.

Encipherment by system squares remained the same save that in some cases the squares were now changed every month.

Compare Appendices 6 and 6a.

In contrast to the army and airforce which down to 1943 had one common operational system with daily change of key for each individual network, the NKVD organs, in those days the several border guard districts, almost always had their own operational system. Later on the designation operational system was only appropriate to a limited degree for these systems of the individual border guard districts. Although the border guard Kasakstan from 1935 on had in addition to the operational table a 4-place simple code

(see substitution systems) which as far as content was concerned far exceeded the limits of an operational system, all the other border guard districts, some of them down to 1939, had to use a simple system, the operational system of the moment, for all purposes. The substitution of the border guard districts North, Leningrad and Kasakstan and that of the coast guard district Novorossijsk where the same in structure and use as the operational systems of the army. The only difference was that the system of the border guard districts North, Leningrad and Kasakstan had instead of two digits a digit and a letter as cipher elements.

The system of the coast guard Odessa and in particular that of the border guard Kasakstan were already more advanced, the former was complicated by using a null, the later by transposition.

For encipherment of the text and of the call signs, system squares like those of the army and airforce were employed. For the mixed elements used by border guard districts North, Leningrad and Kasakstan two system squares were required, one with digits and one with letters.

Compare Appendices 7, 7a, 8, 8a, 9, 9a, 10, and 10a.

(Operational and general systems of the border and coast guard district).

Not until 1939 was a common substitution system similar to that of the army and airforce introduced as operational systems for all NKVD organs. Since the structure and use of this new system, which was intended only for operational and tactical traffic, almost completely correspond to that of the PT--35 of the army and the airforce, we can dispense with any fuller reproduction.

Regarding the substitution systems for operational use we may say in conclusion that these almost always involve cipher groups of two values -- 1 digit or 1 letter for the horizontal and vertical coordinates, which were combined in the messages into groups of 2 or 4 places and for the coast guard Novorossisk into 6-place groups.

Signal code tables did not appear in the Soviet Union until the second half of the war. These were 3 and 4 place systems of slight extent which fall under the heading and type SUV and were used exclusively by armored units. They contained in addition to a spelling alphabet only one digit numbers and words or phrases important for tank warfare with small and mediumed sized units. In messages of this class unimportant words may be sent in plaintext, simply inserted between cipher elements, map coordinates— generally 5-place -- are disguised by the most varied map or coordinate keys.

Compare appendices 11 and 11a (Schematic presentation of a small tank signal code table and a sample message).

It was very rarely possible to work out such tank tables completely, frequent change of key and often very slight traffic greatly hindered decipherment. Yet in most cases even fragmentary reading could afford valuable hints.

Since in general addresses and signatures spelled out in letters or syllables afforded the most important starting points for unauthorized decipherment, the enemy began in 1943 to encipher these addresses and signaturesin messages in the SUV systems with special address and signature codes quite different from the text. These supplemental codes which were issued by a front staff or an army unit contained in addition to simple concepts like "chief", "commander", "leader", or "deputy"

composite concepts such as "chief signal officer" and in the address code of an army unit such expended concepts as: "commander of the 17th tank brigade" or "chief of staff of the 4th armored army". Interpretations of this last type were difficult to reach and could only be risked after very careful, intensive study of the traffic involved. With interpretations of this sort decipherment has to assume a great deal of responsibility because an error of interpretation not only gives the wrong ordinal of a unit but may mislead regarding the direction of attack, the target, the point where the attack is to begin and the momentary base of the unit involved. Concepts like those of an address code only occur as such and cannot be checked by the context elsewhere. It was particularly difficult to solve encipherments of such address codes but nevertheless good results were achieved.

Without question the great majority of all deciphered Russian systems belongs to the class of so called substitution systems, including codes, code tables, small and very small codes, and expanded substitutions (Cäsar). Systems of this type appeared in Russian use from the beginning of our observations and although they were mostly quite primitive when compared with Russian systems of 1945 it may be worth while to sketch them. This appears all the more necessary since systems of this kind, although sometimes with difficult encipherment, could be broken and read currently down to the very day of capitulation.

A few words regarding the term substitution system [Tauschverfahren].

Although this technical expression like all others is explained in the appendix [20], it will be taken up here in the text because the interpretation contradicts the strict meaning. In general all replacement

systems are substitutions since in place of the letter, syllable or the word in the plaintext, a cipher element, i. e. some combination of digits or letters is written. Or to put it differently the plain element is exchanged for a cipher element. In technical language only those substitutions are called Tauschverfahren where the structure represents an advance over the simple substitution (Cäsar) and where in particular the reincipherment goes beyond the framework of a simple letter-for-letter exchange and provides for substitution of bigrams, a mixed substitution—letter (or digit) or a multiple (at least 3-fold) substitution of monograms, e. g. with 3-digit numbers — cipher elements for hundreds, tens and units. The first system which could be worked out fairly complete was a general airforce code used in 1935/37 with approximately 1000 groups.

Compare Appendices 12 and 12a.

The encipherment of the systems merely covered the 10 pages, each of which could be expressed by from 2 to 10 different 2-digit numbers, while the basic code numbers of the individual positions remained unchanged.

Change of encipherment resulted irregularly and at different times in different districts and networks. The amount of material intercepted in this system also varied greatly. In the winter months often for days at a time no messages were transmitted, while in spring, summer and fall several nets (military districts) worked simultaneously with this system although with different encipherments.

Other airforce codes of like character appeared yearly around the first of May and remained in use for a short time, approximately 1 month. In all probability these were used for practice at the maneuver-like air

parade held on the first of May in Moscow. With them were enciphered starting and landing reports, weather reports, operational and traffic messages of air units coming and going from all parts of the Soviet Union. When these systems were used it was possible for the first time to note increased ground-air traffic in cipher. These were always 3-place systems with 500—600 groups and alphabetic structure. Encipherment was by single digit substitution in the 3-digit element.

Aside from a number of other small and medium codes used for a short time during various maneuvers and exercises of the airforce in all military districts, the last air system of this kind, the VAK — 38 = ВАК ВОЕННЫЙ АВИАЦИОННЫЙ КОД-38 = airforce code of 1938 deserves special mention. This 3-digit code with some 800 groups contained letters, words (no syllables!), cover groups for types of planes, numbers, punctuation marks and compound concepts like "plane has made emergency landing" or "airfield unsuitable for landing". This could be transmitted with anyone of 3 basic encipherments designated by the colors black, red, and green and with additional encipherment by 2-digit substitution for the hundreds and ten (elements A and B). Element C (unit remained constant in the basic encodement.

Compare Appendices 13 and 13a.

This system, used from 1938 to the end of 1939, represented an advance over its precedessors. Since 1939 systems of this kind no longer appeared as general systems of Soviet flying units.

In contrast to the airforce which had had systems like those just described since 1935, a general system did not appear until 1937 in the army.

Up till then a relatively large army code was known only in the military district of Moscow. This contained 20 pages with 100 groups each and was therefore twice as extensive as any air code known up to that time. Of terminologic-alphabetic structure [group numbers in natural sequence and vocabulary in alphabetic sequence] this 4-digit code was enciphered by 2-digit substitution for elements A and B (thousand and hundred) by a single digit substitution for element C (ten), while element D (unit) remained unchanged.

Since a full description of each individual known system, even those of greater size, would take too long, only one of the best known, a 4-place combined army air force code will be described in detail.

The first general army and air force system of considerable size was the 4-digit code with some 4600 groups in the military district Volga which first appeared in connection with a maneuver. The encipherment of this code and of its successors — codes OKK-5 to OKK-8 — was by the aid of 2—digit substitution sequences or tables for elements AB and CD. Usually 2 indicator groups showed the sequences selected and the starting points.

Compare Appendices 14 and 14a.

The OKK-5 = ОБЩИЙ КОМАНДИРСКИЙ КОД-5

= general commander code—5 with 50 pages of 100 groups each was so extraordinarily well composed that its successors show only slight changes. The use and swiftly following replacement of 4 large codes in the course of the years 1939-1941 is explained by their capture. The OKK-5 was captured in the Russo-Finnish war, codes OKK-6 to OKK-8 in the Russo-German

war. However all these systems had been recovered analytically and were read completely before capture.

The last substitution system on a large scale to be used was the OZKK-7 = ОЦКК-7 = ОБЩИЙ ЦЕНТРАЛЬНЫЙ КОМАНДИРСКИЙ КОД-7 = general central commander code-7 which was employed in the rear area and yielded very valuable hints regarding supply and new formations of the enemy. It was enciphered with 2-digit substitution tables like the systems just described.

All systems with the designation SUV belong without exception to the substitution category. After decentralization of Russian cryptography great latitude was given individual fantasy and initiative through the fact that the signal officers of every division, indeed of every regiment, were able to compile and develop their own systems for their own areas. Aside from a number of "stilistic flowerings" in the development of SUV systems — especially in the beginning, changes were made ultimately which deserved serious attention and represented very considerable advances in security in comparison with the earlier small substitution systems. Above all the basic change from a simple to a two-fold manner of reading greatly limited the possibilities of decipherment and a large amount of traffic became necessary in order to force an entry. The two-fold manner of reading consists in introducing 2, 4, 6, ... to 20 switch groups of which one half signify "read the first letter of the word", the other half "read the entire word". This made it possible to use any word as its initial letter. Thus the hitherto customary spelling alphabet could be dispensed with, the peak frequencies of individual letters disappeared, the frequency curve flattened out.

The great number of SUV systems differing with respect to size, structure and encipherment makes it impossible to describe them individually. It will suffice to give one example and to state that of all the changes the two-fold manner of reading is the most important and most fundamental innovation.

Compare Appendices 15 and 15a.

Relatively large substitution systems of the NKVD appeared considerably earlier than those of the army and airforce. The first, a 4-place code of some 25 pages with 100 groups to the page, was in use from 1935 on in the border guard district Kasakstan where the border troops were often isolated in winter due to frequent disturbances of telephone and telegraph wires by snowstorms and where news reports were often received in this code. Thus for instance early in 1936 a speech by Stalin which had been printed in "Pravda" and in "Krassnaya Svesda" (Red Star) was transmitted to the border units of Kasakstan by radio as a cipher message. This message, some 1800 groups long, was recognized as having been enciphered by a code which had not yet been extensively broken and the content was soon identified by samples as that of the printed speech. Our very imperfect knowledge of the code was thus materially expanded. This example of an incomprehensible idea of the actual purpose of enciphered radio communications best shows the naivete and unconcern of those responsible. This system, as the first major substitution system, was enciphered by a 2-digit substitution which changed approximately every week.

The three 4-place codes which occurred down to 1939 and had up to 5000 groups were enciphered by 2-digit substitution sequences or tables exactly like those of the army and airforce. It is worth noting that one of these codes with some 3500 groups was the so called reserve system and appeared occasionally in various districts down to 1943 when regular cipher materials were missing.

In 1939 the first general NKVD code was introduced with 10,000 groups, 100 pages each with 100 groups. This system which was used by all border guard districts of the NKVD, the interior troops NKVD and by all other NKVD organs whether military or political, was enciphered originally by single digit substitution in three phases and later by additive sequences (see NKVD additive systems).

Encipherment by single digit substitution in phases:

After the text has been encoded, this intermediate text consisting of the basic code groups is enciphered digit by digit in three phases.

Example:

Substitution table for 3- phases

	0 1 2 3 4 5 6 7 8 9	Digits of the basic code
a.	7 9 3 4 1 0 8 2 6 5	Encipherment, phase 1
b.	3 6 1 8 7 2 9 5 0 4	Encipherment, phase 2
c.	0 4 6 5 1 3 7 9 2 8	Encipherment, phase 3

Basic code groups:	3512	4278	9310	6264	0786	....
Phase division:	abca	bcab	cabc	abca	bcab	....
Enciphered text:	4243	7620	8460	8171	3969	....

At the time of capitulation three 4-place codes of the NKVD border guard and security troops were in use and as many as 200 messages in these systems could be read daily. These were code tables with 2000 to 2500 groups of which Serno = ЗЕРНО and NIVA = НИВА were enciphered by 2-digit substitution and Visa = ВІЗА by a mixed substitution (2-digit and 1-digit). For work with Serno each of the more than 30 different nets had 20 encipherment tables, 10 each for the pages and the groups. By ten different possibilities of sliding the groups of the individual pages with respect to one another $10^3 = 1000$ different encipherments could be used on each net. An indicator group, position differing on each net but among the first ten groups, showed by its elements A, B and C the group encipherment, slide and page encipherment. Element D was usually a blind, often a null.

Compare Appendices 16 and 16a.

The encipherment of code table Niva was similar and was also indicated by an indicator group whereas with table Visa the encipherment was less complicated but was not shown by an indicator group. The substitution tables were changed within the nets about every three months. We may mention further that code table Niva first appeared in January 1945 and had been almost completely recovered by the author by the end of February. It would be conceivable, in view of the long life of NKVD systems, that this code is still in use (July 1947).

As the last major substitution system of the NKVD organs reference may be made to the 5-place railway code NKVD containing 2500 groups on 25 pages with elements AB and DE enciphered by 2-digit substitution

sequences and element C enciphered by 1-digit substitution. This code likewise was in use down to the day of capitulation. With 25 pages of 100 groups each it was possible to express every meaning of the basic code in several ways in an encipherment and thus to prevent repeats.

Example:

For each of the 25 pages (AB), 01—25 in the basic code, there were 4 possible expressions with 100 different dinomes (00—99) within an encipherment. The middle element C divided each page into 4 quarters and indicated the quarter used. Consequently with 10 digits (0—9) two quarters could be expressed in two ways and the other two quarters in 3 ways. Hence there were either $4 \times 3 = 12$ or $4 \times 2 = 8$ ways of expressing one and the same basic code group in any encipherment.

Aside from the larger code described, smaller, usually 3-place codes were occasionally broken and read, among others a system of the convoy troops NKVD. These codes regularly showed the same structure as like sized codes of the army and airforce.

Pure transpositions, were only used in the army and airforce for practice purposes, in particular as training for a line planned in 1937 between the Soviet Union and Czechoslovakia. The content of these transposition messages was pure propaganda text.

Letter transpositions such as were used for practice in the army were never found in NKVD traffic. However a transposition was used as encipherment of a 4-place code with 10,000 groups in the Arctic district and along the Finnish frontier in 1943/44. This system was broken and read in part.

Regarding the use of transposition systems on a large scale reference is made to the discussion of partisan, scout and agent systems later in

in this report.

Basically the 5-digit Code Chiffre, also called operative code, served for the transmission of radiograms of operational and tactical content, i. e. those concerning upper level command, in the networks of the higher and highest command (from the brigade or division staff up to the general staff of the RKKA). The Chiffre code or simply the Chiffre was systematically altered in vocabulary to meet changing needs and to improve it with respect to cryptographic security by more and more consistent use of variants for frequent meanings (punctuation) as years went on. These new editions of the Chiffre came during the war at intervals of 6 to 12 months whereas in peacetime--in so far as a Chiffre was used at all--the same code was probably employed for longer periods, presumably 2 years at the least. The first 5-digit Chiffre appeared during the Polish campaign and the period of occupation of the Baltic countries, Roumania and of the Russo-Finnish war. The original designation of this code, which was recovered and for the most part read by our signal intelligence, never became known; it was withdrawn in the spring of 1941 and was never captured by the Germans. At the beginning of the Russo-German war code 011-A was in use. This was replaced by codes 023-A, 045-A, 062-A and finally by 091-A which remained in use until the capitulation of Germany. Aside from these 5-digit operative codes a lot of other 5-digit army and airforce systems were captured which were either reserve systems or, having been distributed to the troops, fell into enemy hands before being put into use. All these codes except code 045-A, which was in use from March 1942 to March 1943, were alike in structure except for the progressive vocabulary expansions and improvements

mentioned above. They consist of a text part and a special part, the arrangement is alphabetic. The general part contained letters, bigrams, trigrams, syllables, words, compound concepts, phrases and entire sentences in a strict alphabetic sequence with punctuation marks, fractions and ordinals, hours and minutes, numerical designations, armies and divisions, day dates, year dates, and caliber designations scattered throughout the entire part. In the special part these concepts, which were out of alphabetic sequence in the general part, were assembled by group numbers to facilitate finding. Code 011-A had some 19,000 meanings on some 390 pages. The systematic structure of codes of this kind meant that the number of groups increased with each new addition. The last known code 091-A had some 23,000 meanings on 430 pages. Despite the insignificant expansion its perfection was considerable from the standpoint of decipherment. For the analyst the chief points of attack are the frequency peaks occurring in the text and conditioned by the language itself. These include especially marks of punctuation (period and comma, which with some 6.5% and 4% topped the frequency curve of Russianmilitary text of the content met in Chiffre code). While these concepts were represented by single groups in code 011-A and therefore offered the analyst good points of entry, the number of groups assigned them increased with each new edition of the code and in code 091-A there were approximately 350 groups for each of these two marks of punctuation. This forced the analyst to change his method of breaking-in and to use more laborious means. These new means will now be described briefly: aside from the marks of punctuation there are in Russian, particularly in military text, frequency peaks which can be picked out even when enciphered by syllables or by complete words. We are concerned with single letters which in Russian have at the same time the significance of prepositions

and/or connectives. These are the letters: И = and, С = from (since), А = but, К = to (to the), У = at [with] and В = in (in the).

Our decipherment developed new possibilities of breaking-in to this last 5-digit code by making use of this fact even though with the most frequent of these letters the И for instance the Russians had made a subdivision into И = letter, И = final letter, and И = connective. A further frivolous handling of punctuation which was discovered later further expanded the possibilities of breaking-in. In practice each page of the code (except the special part) contained both a comma and a period. If for instance the Russian had transformed the word "НЕТ" into a cipher element and wished to follow with a mark of punctuation, for convenience sake he took that period or that comma which stood on the НЕТ page of the code. Since this practically became a rule it was possible to draw deductions regarding page numbering in the basic code from a punctuation mark which might possibly be discovered, these deductions relating to the page [of the group] ahead of the punctuation and also to the vocabulary items on the page. An exception to the series of strictly alphabetic Chiffre codes was code 045-А as mentioned above. This code showed interrupted-alphabetic structure. For a skilled analyst this hardly meant any greater difficulty. It is interesting to note that whereas all innovations in the Chiffre code were so promptly captured that the originals were almost always in our hands when the Russians put them into use and that therefore the necessity for code recovery dropped out, precisely the more difficult code 045-А was not captured until about 3 months after it was introduced by the RKKA. In these 3 months in spite of the fact that its structure differed from that of its predecessors it

was so far recovered that it was already possible to read some parts of messages enciphered with it.

The Russians attached no particular significance to the loss of a Chiffre code, not even to its capture by the enemy, since they think that the system of encipherment affords full security even when the code itself is in enemy possession.

This method of encipherment consists in the addition to the 5-digit code groups of 5-digit additive groups from a practically endless, random additive sequence (so called Gamma table). The tables used with the Chiffre code can be divided into 2 categories according to use:

1. General tables, containing 300 5-digit additive groups. At the top and on the side of the table are 2-digit column indicators and 3-digit line indicators, which permit the cipher clerk to show by the coordinate principle the additive group with which he starts. In the general tables therefore encipherment may begin at any desired point in the table but must then continue serially until the last group of the text is enciphered.

2. Other tables with different names according to their use but all alike in the method of application. With these tables containing 60, 80, or 120 5-digit additive groups enciphered must always begin with the first group of the table and continue serially. When one table is used by the next is taken automatically.

The general tables are regularly used for one day in the area of a unit and its subdivisions (e.g. in the traffic of a front staff with its army staffs or of an army with its divisions and brigades.) The

purpose of such tables is the transmission of messages whose content is intended simultaneously for several addresses (hence the designation "general"). All other tables serve for communications between two partners: the army with one of its divisions, the front staff with one of its armies, etc. These tables, designated therefor "individual tables", are only allowed to be used once in contrast to the general tables which may be used a number of times during one day, since in the later case security is assured by the possibility of using different starting points. The individual tables bear different designations according to the range of use, e. g. AKORD (army-corps-division), FAK (front-army-corps), CC = СВЕРХ СРОЧНЫЙ E = most urgent, O = ОСОБЫЙ = special and circular. From the point of view of decipherment they all belong to one category, namely individual tables, since they are intended only for individual one time use. This one time use means an extraordinarily great demand in the RKKA for these means of encipherment. They are produced in the 8th Section of the General Staff of the RKKA and are bound up into BLOKNOTS [blocks] with 31 general tables or 50 individual tables to the block, these are then delivered to the front staffs. From here distribution to the army staffs was made and these in turn supplied their divisions and brigades. It is worth mentioning that the supply of such means of encipherment to the troops never failed even in the most critical period and that there were always enough reserve blocks on hand.

Important is the observed trend of the Russians away from the general to the individual tables because these later when used once according to instructions afford absolute security against unauthorized decipherment whereas when there was enough traffic general tables could be recovered

almost throughout the duration of the war.

The principal role in the encipherment systems for all major codes including those of the NKVD is played by the additive sequence which appeared for the first time in this connection in 1940 and has since been employed in all manner of variations.

The first additive sequence was prepared from the book "History of Leninism" by Josef Stalin by the use of a letter conversion table and this additive was used to encipher the 4-digit code mentioned among the NKVD substitution systems originally enciphered by a single digit substitution in phases.

Typical letter digit — conversion:

И, Щ, Э = 0	С, Б, З = 5
О, Ж, Ф = 1	А, У, Ы = 6
Е, Х, Ь = 2	В, Р, Ю = 7
Н, Г, Ш = 3	К, П, Й = 8
Т, Д, Я = 4	Л, М, Ч, Ц = 9

Letters of the text were converted into digits by the above table, the starting point in the resulting additive sequence was given as an indicator group namely the page (01—99) and the line (01—45). The key for this conversion table was so constituted that the procentual frequency of the letters equated to a digit came to about 10%. This assurred that no digit (0—9) showed any frequency peak.

Example of conversion:

We will assume that the following Russian text is taken from "History of Leninism" and stands there beginning with line 27 on page 34.

Then the indicator would be 3427.

The conversion of the letters into digits, i. e. the make-up of the additive sequence, would be as follows:

Н	Е	О	Б	Х	О	Д	И	М	О	З	Н	А	Т	Ь	Ч	Т	О	К	А	Р	Л	М	А	Р	К	С...
3	2	1	5	2	1	4	0	9	1	5	3	6	4	2	9	4	1	8	6	7	9	9	6	7	8	5

Translation: ... it is necessary to know that Karl Marx...

Study by our cryptanalysts of the recovered additive finally made possible recognition of the additive as converted letter text, due to rather long repeats, and to solution of the key. On the basis of recovered fragments of text it was then possible to guess the book used for the purpose.

In 1942 another NKVD code for interior troops was enciphered in similar manner. The basis for production of the additive was in this case a military manual, "signal intelligence service".

The border guard troops NKVD on the frontiers of neutral countries produced their additive encipherment, so far as the author recalls, by 20 + 4 digit sequences whose displacement with respect to one another was expressed by means of an indicator group.

The double additive which was in use at the last (simple additive down to the end of 1944) using Gamma tables concludes our survey of the development of additive enciperments of NKVD systems. With this last method of encipherment there was a decidedly clever camouflaging of the indicator groups so that these were especially difficult to recognize and were only comprehended relatively late. The camouflage follows different formulae in each network.

Example of disguise of indicator groups:

Assumed cipher text:	2739	1825	7930	8221	1975
	6308	2649	2314	5539	....
	....	....	....	....	....
	etc. to		4199	1537	2811
	3081	6275	0185		

Formula: A1 - A4 S5 + S3

(A1 means the first group, A4 the fourth group from the beginning; S3 is the third group from the end, S5 the fifth from the end).

Indicator (according to formula): 2739 - 8221 = 4518 (mod.10)

Control group (according to formula): 1537 + 3081 = 4518 (mod.10)

Here both A1 and S3 are inserted groups without textual meaning, their position in the message is shown by the final group.

Final group: 0185 (ABCD) where A + B indicates the position of the first inserted group, C - D that of the second.

Since with the double additive as with the former single additive the same gamma tables were used several times, the encipherment of 50—75% of all messages could be removed and the content read after recovery of the code. The actual 4-place codes, 3 in all, were 2-part codes. The encipherer therefore needed a copy — Chiffrant — with the entries in strict alphabetic sequence, the decipherer needed a copy — Dechiffrant— with the code groups in strict numerical sequence. The breaking of such systems, quite apart from the difficulty of an additive encipherment, is very laborious and is only possible by numerous comparisons which must be set up in the form of chain statistics.

In conclusion it must be stated that the advanced status of decipherment of precisely these very difficult NKVD systems is to be ascribed in large

measure to the fact that they were worked on centrally, i. e. exclusively in the office of the "General der Nachrichten - Aufklärung" and therefore an increased degree of secrecy was assured. From the very fact that NKVD systems almost always remained in use for more than 2 years it must be concluded that the Russians considered it impossible for unauthorized persons to read them.

Especially varied in structure are the cryptographic systems of partisans, scouts, and agents. In contrast to army, airforce and NKVD, numerous transpositions — single and double — appeared, less often grills. In the main the use of transposition for these circuits is due to the fact that their use avoids the necessity of carrying along written material. For single transposition it is only necessary to remember a key word, for double transposition two key words, by the aid of which the numerical key can be produced at any time. In contrast to the army, airforce and NKVD which required extensive well developed cryptographic systems for their uses, for the traffic of partisans, scouts and agents minor systems, usually with difficult encipherment, serve the actual purpose better. A frequent change of key, in this case a change of system, can be accepted more readily here than with the army and air force and especially with the NKVD since here only two or at most a few stations are forced to use the same cipher while particularly with the NKVD the entire organization for the whole great country uses a system for a rather long time even though with different encipherments. It would lead too far afield to reproduce all types of ciphers which were recognized, worked on and decrypted, hence only a few examples of characteristic types will be given.

Compare Appendices 18a--d.

In transmitting place names, areas of attack, commitment and assembly the Russians in army and airforce traffic made use of 5-place coordinates (Gausz--Krüger), which were inserted in the message text after being specially enciphered. Before the war a planshette [mask] of celluloid was devised for this purpose which made it possible to pin point areas of 1 square kilometer, or by adding a 6th digit (1--9) or a letter (a--i) areas of 333 square meters (1/9 square killometer). On the maps with scale 1: 100 000 used for the purpose a 2-digit number was printed alongside cities with a population of 10,000. In as much as only 100 such numbers (00 -- 99) were available, these necessarily had to be repeated many times in view of the size of the country. However the general area in question, in most cases the map sheets, was known to the enciphering and deciphering clerk in advance. The numbering ran in strict numerical sequence from left to right and from top to bottom over the entire European portion of the Soviet Union.

Compare Appendices 19 and 19a.

After the outbreak of the war the Russians had to count also on the capture of these coordinate encipherments and was therefore obliged to adopt another diguise. In the long run the various units enciphered the coordinates differently, the 1: 100 000 maps with printed numbers beside the names of cities with 10,000 or more inhabitants went out of use.

One of the most frequent methods of encipherment became now the symbolic [mod 10] or arithmetic addition of two dynomes, in the latter case omitting the hundreds, to the AB and CD elements of the 5-place

coordinates leaving the final element E unchanged. Map reading after decipherment was in the usual order — left (right) then upper (lower) margin — the final unenciphered digit of the coordinate gave the subdivision of the 1 square kilometer area.

In contrast to army and airforce the NKVD organs used 4-place coordinates, i. e. without any subdivision of the 1 square kilometer area. The lack of 1: 100 000 maps for the Balkans, Hungary, Croatia, Czechoslovakia and South Poland caused the use of 1: 300 000 maps where the 4-place coordinates designate an area of 3.3 square kilometers. The most important differences in the coordinate data between army and airforce on the one hand and NKVD on the other lie in the fact that the former disguised the coordinates separately while the NKVD organs encipher them along with the text and furthermore in the fact that army and airforce transmit either separately disguised coordinates or place names enciphered in the text, while the NKVD formations regularly give both the place and the coordinates one right after the other and encipher them in the text. Only in one case does the NKVD omit the names of places lying in the coordinate area namely when areas are involved, such as rather large forrest areas, which are bounded by several successive sets of coordinates.

The so called verst maps which were used in 1937/38 are no longer employed. In general the Soviet armed forces employ today only maps 1: 100 000 and 1: 300 000.

The herewith concluded main section of the report with its numerous appendices has been concerned with the development of Russian military and political cryptography. The author requests once again that the reader bear in mind that it is extremely difficult to explain more or less

scientific material to those not familiar with the subject without being boring and going into too great detail and yet to do justice to the facts although writing purely from memory.

Part III

Structure of the Russian Cryptographic section in the former German Army and a criticism of its organizational defects.

A. Introduction

B. Organization of the cryptographic section (Russia) and its employment.

C. Cryptanalysis — Russia

1. Short review of the development of cryptanalysis — Russia.

2. Personnel and performance.

3. Top direction and results of analysis.

4. Selection, training, and employment of cryptanalytic personnel.

D. Criticism of organizational defects.

Signal intelligence arose in connection with the development of radio in its early stages and under very different names in the years of the first world war. Its significance especially in Germany, was at the outset quite problematic. In contrast to Great Britain where the British Admiralty for example was able to achieve outstanding results in the course of the engagements in the North Sea, in the first phase of the battle of Skagerrak (Fleet— Grand Fleet and High Seas Fleet), the German units were only able to score occasional successes in the last two years of the war. Signal intelligence, still new and not well organized in its needs and duties, was at first a purely experimental thing and was often termed mere play since practical results were rather rare.

Only the further development and utilization of radio for all purposes of communications, both in war and peace, for military, diplomatic and economic purposes, gave signal intelligence an increased importance and finally permitted it to become one of the most important, in any case one of the most reliable of the intelligence organizations.

Unfortunately there are even today a great many people in important military and political capacities who, whether from ignorance, disbelief or plain antipathy, ignore the significance of signal intelligence, especially that of cryptanalysis, and prefer to trust the instable, often indifferent reports of agents and spies. This attitude has had, as will appear, disastrous consequences for Germany's conduct of the war.

The organization of signal intelligence properly divides into 4 groups or parts of which each part assumes a number of functions while all are most closely coordinated with one another. Even though the assignment of each of these parts is perfectly definite, nevertheless in judging the entire apparatus and in the employment of each individual part the organization as a whole must be taken into account. Just as the final part, content evaluation, arose when decipherment could achieve practical results, decipherment only became necessary -- or could only function --, when it was possible to supply for decipherment not merely individual messages intercepted at random but the entire traffic of recognized networks and circuits are at least substantial quantities of this traffic. This recognition and ordering of networks and circuits in its turn presupposed the clearing up of operational signals, of call signs and wave lengths, and was based naturally enough on message intercepts, i. e. on the intercept service itself. But from this fact--the rise of traffic analysis from the intercept service, the employment of decipherment on homogeneous, quantitatively adequate material, made possible by traffic analysis, and the creation of a content evaluation on the basis of the practical results of decipherment -- can be adduced the necessity for considering the whole, the indivisibility of all four parts.

The following chart shows the duties of the individual parts or groups of signal intelligence and also the coordinated employment of the parts.

	Assignment	Organization
Group 1	Interception	Intercept service Search Cover
	Direction finding	Direction finding Attempts at location
	Training of intercept operators	
Group 2	Traffic analysis	Net analysis
	Coverage and control analysis	Study of radio operations Recovery of call sign systems, wave and frequency allocations.
Group 3	Cryptanalysis	Work on the decryption of messages. Study of cryptographic systems Development of cryptanalytic aids.
	Scientific studies	
	Linguistic studies	
	Training of analytic personnel	
Group 4	Content evaluation	Translation of messages Tactical evaluation Operational evaluation
	Card files	File of names File of troop units File of abbreviations
	Map material	

Liaison with General Staff 1c("Horchlage")

At the head of the former German signal intelligence stood as directing command the General der Nachrichten-Aufklärung (formerly LNA = Leitstelle der Nachrichten -- Aufklärung, still earlier H.L.St. = Horchleitstelle). In operations against the USSR since the beginning of the war or during the course of the war there was subordinated to this top office in respect to functions and personnel 3 to 5 NAAS = Nachrichten-Aufklärungs-Auswertestellen (Horchkommandeure) and 1 Nachrichten-Abteilung in Finland.

Compare part Iv, Appendix 24 (Employment of signal intelligence against the East).

The signal intelligence evaluation centers developed out of the fixed intercept stations which had operated in peacetime (formerly Feste Funk-Empfangsstellen) at Breslau, Treuenbrietzen (earlier at Jüterbog) and Königsberg.

Subordinate to the NAAS, which generally were located at the headquarters of the army groups, were fixed intercept stations (only with NAAS 2), intercept companies and long range reconnaisance [intercept] platoons. While the fixed intercept stations and long range platoons were generally not subdivided, the intercept companies employed close range reconnaisance [intercept] platoons and D/F platoons further forward.

The close range intercept and D/F platoons, whose business was the reception of enemy radiograms according to directives of the intercept companies and the location of unknown stations by D/F, sent their intercepts to the intercept companies without working on them, the intercept companies attempted decryption of the simplest systems and sent to the NAAS material they could not solve.

The fixed intercept stations and the long range intercept platoons were pure intercept stations located farther from the front, they worked primarily according to directives of the General der Nachrichten - Aufklärung transmitted to them through the NAAS. The intercepted traffic was sent to the NAAS.

The duty of the NAAS was the decipherment and the evaluation of messages delivered to them by their subordinate organizations or intercepted on the spot. For this purpose the NAAS had considerable numbers of analysts available whose duty it was to work on lesser and medium difficult systems of the army and airforce and to report the contents of such messages via Evaluation to the "Ic" [G-2] of the army group as well as to the Evaluation Section of the General der Nachrichten-Aufklärung. The cryptanalytic work of the NAAS was directed by the cryptanalytic section of the General der Nachrichten-Aufklärung which also kept the NAAS posted on advances in cryptologic science.

The activity of the section in Finland corresponded in general with that of the NAAS but this unit was smaller and coordinated its work in certain matters with the Finnish army section for Russian cryptography.

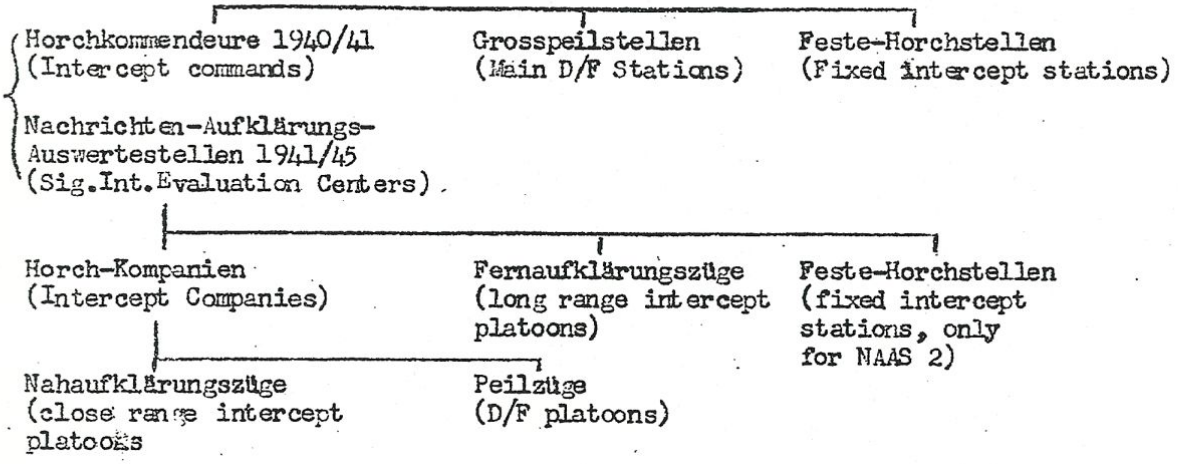
All traffic from the NAAS and the Finnish section was sent in carbon copy with the notation "worked on" or "not worked on" to the General der Nachrichten-Aufklärung. All 5-digit messages of the army, airforce and NKVD as well as all material recognized as coming from the NKVD was worked on exclusively at the central office of the General der Nachrichten-Aufklärung. The purpose of sending all messages which had already been worked over to the central office was control of the cryptographic activity of the NAAS, with direction and assistance were needed.

The results of all deciphered messages were issued daily by the Evaluation Section of the central office in a report "Horchlage" and handed to the interested parties. Included in the distribution were among others: Chef HNW Heere's-Nachrichtenwesen [Chief Signal Officer]), Operations Section, Foreign Armies — East and the cryptographic section of the Airforce High Command. This report, consisting of deciphered and translated messages ("WN. - Meldungen") and evaluation of content, direction finding, and traffic analysis, was sent by courrier classified "Geheime Kommandosache" (the highest degree of military secrecy).

During the war (1943) certain defects in cooperation between the office of the General der Nachrichten - Aufklärung and the NAAS, discussed in more detail in the criticism, caused the setting up of two fixed intercept stations directly subordinated to the central office.

Chart of Signal Intelligence-Russia in the former German army.

Central office (Horchleitstelle 1939/40;Leitstelle der Nachrichten—Aufklärung 1941/44;General der Nachrichten-Aufklärung 1944/45).



Down to 1939 the following fixed intercept stations were employed against the East:

1. Fixed intercept station Treuenbrietzen (USSR and Poland)

   Radio security stations: Schneidemühl, Schlochau, Pasewalk, Meseritz and Fraustadt.

2. Fixed intercept station Königsberg (USSR, Poland and Baltic countries).

   Radio security stations: Neidenburg, Lyck and Tilsit.

3. Fixed intercept station Breslau (USSR and Czechoslovakia)

   Radio security stations: Glatz, Kreuzburg, and Glogau.

Within the signal intelligence service there has been from the start a conscious or unconscious quarrel, a constant competition, between intercept service, traffic analysis, cryptanalysis and evaluation of content. Each of these four parts claims for itself prime significance and importance. It is quite idle to discuss this quarrel which was caused solely by a craving for appreciation. Looked at objectively it can be seen that all four parts are of value only as a unit, i. e. that each part is directly or indirectly dependent on the others and will always remain so. The observations at the beginning of this paper may serve as proof and explanation of this statement.

On the other hand it can be established that the type of personnel of at least three of the four parts is entirely different, or at least ought to be.

While it is quite possible that a good intercept operator after years of experience at the receiver may becom a good traffic analyst, the other two parts, both cryptanalysis and content evaluation, call for entirely different knowledge and essentially higher general education.

It is practically inconceivable that the traffic analyst should not have been an intercept operator or at least a radio operator. Knowledge of details of reception and experience with the routine are prerequisites for a successful traffic analyst, to this should be added if possible some experience in direction finding and technical knowledge of various instruments. Technical and practical experience and long practice are for the intercept operator and for the traffic analyst more important than any theory.

Cryptanalysis calls for good linguistic knowledge on the part of translators and translator-decrypters and good mathematical knowledge on the part of analysts but also presupposes in both cases an adequate general background, quick comprehension, adaptability, persistance, mental alertness, a certain amount of imagination and an indefinable knack.

Of the content evaluator however one must -- in contrast to previous practice in the German Signal Intelligence -- demand that his knowledge in the general field of military science, of tactics and logistics, correspond at least to the knowledge of a good, experienced officer, better still to that of a general staff officer. Naturally a content evaluator must have a good general background and a sense of responsibility, in addition he must if possible have linguistic ability.

It is not the purpose of this report to describe in detail the entire organization of signal intelligence, hence the neighboring fields, traffic analysis and content evaluation are described only insofar as the requirements of cryptanalysis show direct points of contact with them.

The beginning of analytic activity in the Russian field after the World War 1914/18 falls in the 20's. The efforts of Chi (Reichskriegsministerium) [cipher section -- ministry of war] at that time led to

no noteworthy results since very little material was available. With the growth of Russian military and political radio traffic there came into being in Germany at the then intercept stations, the so called Feste-Funk-Empfangstellen, small cryptanalytic sections, often only 1 or 2 persons, whose work down to the spring of 1939 was subordinate to OKW (Reichskriegsministerium), whereas the personnel was subordinate to the signal intelligence sections to which the fixed intercept stations belonged.

Down to 1935 there were really only three fixed intercept stations for observation of the neighbors to the East and Southeast, namely in Breslau, Königsberg and Jüterbog. During the year 1935 these three stations were given the right to set up a number of so called radio security stations of their own with locations in the areas bordering on Lithuania, Poland, and Czechoslovakia.

Cryptanalytic sections at the three fixed intercept stations were composed of civilians, officials and soldiers, but at least until 1941 assumed more and more a civilian character. This civilian character, especially at Jüterbog (later intercept station Treuenbrietzen) had the advantage that no military service, e. g. drill, roll call, guard duty, was required of civilian employees and therefore their entire time and energy could be devoted to the one task, namely cryptanalysis. As traffic increased, primarily as a result of greater radio activity in the USSR, the need for cryptanalysts, translators and clerical workers increased likewise.

A comparative table showing personnel and accomplishments of the fixed radio intercept station Jüterbog (later intercept station Treuenbrietzen)

for the years 1935—1939 (figures are estimated in round numbers) will make clear the development of the cryptanalytic section and also show the decline in diplomatic traffic and the increase in military-political traffic.

Compare Part 4, Appendix 25

Performance and personnel of the fixed radio intercept station Jüterbog (Treuenbrietzen) together with radio security stations for the period 1935—1939 (assignment: Poland and USSR).

With the creation of a signal intelligence unit of the OKH, i. e. with the division into diplomatic-economic (OKW) and military-political (OKH) assignments, with the increase in the number of messages intercepted and in the results of cryptanalytic activity, the cryptanalytic section experienced a considerable expansion in personnel. Unfortunately however provision for this had not been made in time and so it was necessary to work along in the early years with new untrained helpers and to devote a great deal of time, at the expense of the actual cryptographic problem, to training these people, moreover the work of these newcomers called for constant supervision and correction. This expansion of personnel in the cryptographic section with virtually untrained people, the fateful decentralization — control station, NAAS, NA-Finland and intercept companies—resulted in time in a quite unproductive ratio between accomplishment and personnel strength.

Compare Part IV, Appendix 26.

Personnel strength of the army cryptographic unit Russia contrasted with cryptographic accomplishments (1939—45).

Among administrative authorities, especially in the supreme command itself, the widespread, very erroneous opinion prevailed that personnel strength, more or less without regard for the kind of personnel, was the all important factor of cryptographic success. This layman's view regarding the "Black Art" as cryptanalysis was called resulted in very little attention being given to the actual difficulties while the supreme command not merely regarded disagreeable results of decipherment and evaluation with skepticism but rejected them as untrue and tendentious reports. What fateful results this want of belief entailed can be shown by the following striking events from the field of operation of Chi-OKW and of the [army] control unit of signal intelligence.

1. In the Spring of 1941 the high command of the airforce asked its own airforce cryptographic section and also the older, more experienced cryptographic section of the army (OKH) to report the total strength of the (first line) airforces of the USSR as ascertained from the results of signal intelligence. As I recall, the reports of the army and the air cryptographic section differed by approximately 500 machines. The airforce reported some 11,000, the army some 10,500. This report came back with a notation "absolute nonsense".
2. In the winter months 1941/42 signal intelligence of the army learned of the setting up of new Russian divisions in the area to the east of Moscow, by complete reading of messages the cryptanalytic unit learned the division number, the composition and equipment of the divisions, the name of the military commander, the garrison point and the probable area of commitment. These

intelligence reports were rejected as "nonsensical" (except for OKH) but were fully confirmed by later developments.

3. In the fall of 1942 the cryptanalytic section was able to determine the setting up of new armies (62nd, 63rd, 64th, 65th .....69th) to the east of Stalingrad. Although these observations were constantly supplemented and confirmed, people at the highest level could not make up their minds to believe these reports. Only after the 64th army appeared in a sector of the front near Stalingrad was Foreign Armies - East permitted to enter the other armies (with question marks!) on the chart of the Red Army and to present this at the discussion of the situation at the Führer's headquarters without expecting to be exposed to wild insults.

4. From Turkish diplomatic messages the results of the Yalta conference were presented, shortly afters its conclusion, in the form of a memorial to the Command Staff of the Armed Forces, to the OKW and to the Fuhrer's headquarters. The OKW Cipher Section got back the copy presented to the Command Staff of the Armed Forces with the notation "Dem Hosenscheisser Kettler sollte man doch endlich das Handwerk legen /s/ Jodl". N.B. : "The Führer is of the same opinion /s/ Fegelein".

Note: At a later conference on this subject the Chief of the Cipher Section was informed that this was a piece of Russian Radio deception (!). The original copy was taken into custody by the English at the prison camp Lüneburg.

5. A similar event occurred at the time Rumania quit the Axis. Plans for this became known 3 or 4 months in advance through reading diplomatic messages and the matter was brought to the attention of the appropriate authorities. The reports were called "crazy" at the time and found no credence. After Rumania deserted Chi-OKW was called upon to put all messages on this subject together and present them to the supreme command.

It would be possible to give a number of other similar cases but details are not clear in the author's mind and for this reason such cases will not be mentioned. Although the incredulity at highest levels has already been mentioned in the two foregoing parts of this report, it is impossible to stress the subject often enough. If actual examples are not included until this 3rd part, that is due to the fact that in the last analysis the attitude of the Supreme Command towards Signal Intelligence, no matter whether OKH or OKW, is primarily responsible for the failure to take full advantage of the theoretical possibilities and that mention of the subject, as an influence on development, belongs to this 3rd part.

Cryptanalytic personnel, since all standards were lacking, was selected initially according to points of view which did not meet the requirements. At first it was thought that linguistic knowledge should be the main requirement even for analysts. Experience showed that this view, as well as the thesis advanced by Chi-OKW -- you couldn't tell under 5 years whether a person was suitable for cryptanalytic work -- is erroneous.

It is fundamental to distinguish between analyst and translator. The decipherer is primarily an analyst, hence also a mathematician; the translator is a linguist. When both talents appear in one person without the one overshadowing the other, we may speak of a translator - analyst. These simple observations led to setting up certain criteria and examinations for the selection of replacements. It is not possible within the scope of this report to discuss a detailed plan for methods of selection and training, here again an additional report would be needed to give a well rounded picture of the factors, considerations, experiences and questions involved in what may seem to the layman a relatively simple matter. At any event the method of selection mentioned worked out well on the whole. However the level of the available reserves sank from year to year just as their number decreased. Before the war great importance was attached to general education and new appointees had to present a good conduct testimonial from the police and be vouched for by three reputable citizens, with the beginning of the war these requirements began to be disregarded more and more. In any event after 1941 it was very difficult to select new personnel which even approximately corresponded to our wishes and requirements. For instance it may be stated that of some 250 so-called analysts around the turn of the year 1933/34 perhaps 10% were very good or at least good, and another 15% were suitable translator-analysts and 15% might be considered adequate translators. The remaining 60% can only be classed as clerical-assistants if we apply pre-war standards. The training of analytic personnel took the form of courses which were given in Berlin, initially at the intercept station, later at In— 7/VI and for the most part were conducted by the author himself. After completion of the course, which generally lasted 4 to

6 weeks, the new workers were distributed according to need to the control station, the NAAS with their intercept companies and to NA-Finland. Further training was on the job.

The fact cannot be overlooked that this procedure has a large number of defects but in view of the dearth of time, the urgent and, due to decentralization, far too great demand and to the ever shrinking opportunities for selection, no other solution was possible.

The author's long years in a key position at the central office of the signal intelligence in the former German army gave him a chance to recognize a number of serious defects both in the functioning and in the structure of the organization. The most important, striking defects in signal intelligence generally and in the cryptanalytic section in particular are listed below and will give the answer to some questions which may have arisen in the readers mind. This criticism is general property of all long time specialists in cryptanalysis and in signal intelligence in general.

1. The administration of the central office and of its subordinate units had either no or at best very slight technical knowledge in the field of cryptanalysis and often none in the general fields covered by the work. Hence it was not in a position to afford competent leadership for the entire set up and for its individual parts and was always completely uncomprehending and often uninterested when faced with the problems which naturally arose in the course of time in the various special sections. Hence as a rule it tended to retard rather than to advance the work. There was an obvious effort on the part of the administration to swell the figures for the sole purpose of increasing the administrator's

own personal importance by the size of the units.

2. The want of knowledge and frequently the lack of interest on the part of the administration with respect to the needs of the cryptographic section usually made it hopeless to offer any suggestions whatsoever for changes, readjustments, or reform. Here, as everywhere in the armed forces, only higher military rank carried any weight.

3. The decentralization of army cryptanalysis and of all cryptanalytic effort, which was inaugurated with the beginning of the war, resulted from the desire for recognition, primarily of the intercept commanders. This decentralization resulted in a splitting up of the good men, caused duplication, favored the "paper war", and created lasting friction between different heads, made necessary constant training of new workers and materially endangered security by introducing less and less responsible personnel. With good adequate wire communications (telephone, teleprinter, and secret teleprinter), which are taken for granted today, there is nothing in the way of a centralized cryptanalysis, and even in those days centralization would have overcome most of the defects just enumerated. Although all important analysts repeatedly expressed this view a change could not be effected due to lack of insight at the top.

4. One of the worst faults in the appointment to key positions at the central office and at the evaluation centers was the fact that the Chief of an M.I.S almost always had the rank of colonel

whereas the higher ranking organization had as chief a first lieutenant at best. The consequence was that whenever there were disagreements, questions of competence or the like, the higher rank frequently carried the day. In many cases the NAAS appealed to the area commander [army group], the Central Office to the Chef-HNV as final court of appeal.

5. Due to the fact that the NAAS was physically attached to the command of the army groups a close contact between the "Ic" of the later and the evaluation section of the NAAS inevitably resulted which finally brought it about that the control of the NAAS in technical matters corresponded less with the needs of the central office than to the wishes of the commander. This necessarily led to friction between the NAAS and the Central Office and this often had a bad effect on the results of the work. Thus for instance the NAAS-2 once refused to intercept NKVD radiograms in any quantity on the ground that the content of these messages would not interest the "Ic" of the army group and that furthermore the cryptanalytic treatment of these messages was reserved to the Central Office. This and similar cases forced the office of the General der Nachrichten-Aufalkaldrung to set up 2 fixed intercept stations of its own which should serve only the needs of the Control Office, in order to avoid unnecessarily embittering the relations between the Central Office and the NAAS and because irrational appointments to key posts had made it appear futile

to fight the matter out.

6. The splitting up of cryptanalytic work between the central office and the N AAS with its intercept companies had as a result that, along with a vast "paper war" — 1 original and 2 carbons of every message for the Central Office, NAAS and Intercept company--, there was almost always duplication of effort by the analytic and evaluation sections. It frequently happened that one and the same message was intercepted by the intercept companies of several NAAS and was worked on almost simultaneously in all these units. With the set-up described such duplication was hardly to be avoided.

7. The above criticized duplication of work was not infrequently the result of a completely misdirected ambition on the part of the administration of the individual unit. Conscious of the fact that a particular system was already worked on successfully by another unit, they were determined for competitive considerations to solve the same system and try to dispute the "credit" of the unit which originally solved it. In spite of the regular exchange of solved systems between the individual units by way of the Central Office this could often be done without incurring suspicion of plain cribbing because courier connections were often poor.

8. The worst disturbance of the professional work both at the Central Office and at its subordinate units resulted without question from pure military red-tape. The treatment of the workers was not according to their professional ability and accomplishments but

exclusively according to their military rank, secondarily according to their military bearing. Military service such as drill, target practice or field exercises, guard duty, roll call, even inspection of grounds and quarters were taken so seriously and considered so important that the actual cryptographic work not merely suffered as a result but was sometimes discontinued for hours. In comparison it can be stated that with the civilian character of the organization in peacetime relatively much more was accomplished.

9. The Evaluation Section was made up for the most part of subordinate officials who were inexperienced in theoretical and usually also in practical command and knew little of military science. They often gave free reign to their fantasy and their incompetence and consequently not only evaluated faulily but often drew wholly unjustified conclusions. In addition scarcely one of the Evaluators knew Russian well enough to work with the original text of deciphered radiograms and consequently had to rely on translations which can frequently be misinterpreted, no matter how able the translator.

This enumeration makes no pretence to being complete. The author has merely sketched the most striking and damaging defects. A number of other inadequacies might be criticized but they might not be very damaging to the work itself.

The unmistakable result of all these defects was an extremely unproductive dissipation of energy resulting in a distinct over-organization which ran idle much of the time. With sensible, professional planning it would have been possible to accomplish very much more with a much smaller, better integrated and simpler organization.

To sum up we may repeat and emphasize the fact that the prerequisites for a maximum performance with a minimum expenditure can only be achieved if the following very urgent conditions are met:

1. Close cooperation of all the sections under the leadership of a responsible, active, intelligent person who is interested in the work itself. (It is not necessary that the intercept station be located in the vicinity of the other 3 sections provided there are good wire connections, particularly as the location of the receivers will depend upon intercept conditions).
2. Centralization of cryptanalytic and evaluation work to avoid splitting up [personnel], limitation of the "paper war" and avoidance of difficulties arising from questions of competence.
3. A sensible policy in regard to personnel, taking the point of view that quality takes precedence over quantity, with a resulting assurance of security through the employment of the least possible number of dependable, highly qualified and economically worry-free professional people as guardians of the secrets.

Part IV.

(Appendices)

Aside from the appendices mentioned in the text of the report consisting of schematic reproductions, map sketches, comparative and summary tables, there are three other appendices which may be explained briefly here.

Appendices 21 and 22 give as exact data as possible regarding systems solved or captured which were in use over a long period, appendix 21 covers the peacetime years, appendix 22 the war years. They repeat in general various details of the second section of the technical part in order to give a general survey and a comparison by means of thumb nail sketches. Within the limits of this compilation it is impossible to introduce individually the multitude of systems falling in the category "SUV" (camouflaged transmission of messages of the troop command) and "PT" (chatter tables), all the more so since these were usually short lived and often were only partially broken and some have slipped from my memory. In appendix 22 therefore only the most important characteristics of "SUV" and "PT" systems are included again.

Appendix 23 gives a comparison of three alphabets. The first is the Russian Cyrillic alphabetic, the second is the German (English) alphabet corresponding to the Morse signals of the Russian alphabet and the third serves for phonetic transcription of Russian names of persons and places.

List of appendices

Appendix	Description
1a,b	Area of employment of border guard Leningrad and North.
1c	Area of employment of coast guard Odessa.
1d, e	Area of employment of coast guard Novorossisk and of border guard Transcaucasus.
1f	Area of employment of border guard Kasakstan.
2	Area of employment of NKVD regiments of the border guard and security troops.
3	Table of general types of cryptographic systems arranged with respect to size and to use.
4	"PT--35", first general operational system of the army and airforce with key material for 1 month.
4a	Example accompanying 4.
5	"PT--39" General operational system of army and airforce.
5a	Example accompanying 5.
6	"PT--41" Last general operational system of army and airforce.
6a	Example accompanying 6.
7	Substitution system of border guard districts North, Leningrad and Kasakstan.
7a	Example accompanying 7
8	Substitution system of coast guard Novorossisk.
8a	Example accompanying 8
9	Substitution system of coast guard Odessa
9a	Example accompanying 9
10	Substitution system border guard Transcaucasus.
10a	Example accompanying 10

11	Small tank signal table (SUV system)
11a	Example accompanying 11
12	First general airforce code 1935/38
12a	Example accompanying 12
13	"VAK -- 38" Last general airforce code 1938/39
13a	Example accompanying 13
14	Sample page of "OKK-5" (general commander code of the RKKA) with keys.
14a	Example accompanying 14 (code description)
15	Example of the general SUV system. (regiment)
15a	Example accompanying 15
16	Fragmentary reproduction of code table "SERNO" of border guard and security troops NKVD 1943/45.
16a	Description of code and method of encipherment, accompanying 16.
17	Example of additive encipherment (operational-tactical code general table).
18a	Partisan, scout and agent systems. Sample of a one and two place substitution with example.
18b	Sample of a double transposition with example.
18c	Sample of a grille with example.
18d	Additive encipherments
19	Example of a Russian map planchette (scale 1: 1.5)
19a	The map planchette and its use.
20	Explanation of technical terms
21	Compilation of systems of the army, airforce and NKVD 1935—1941 which were in use for sometime and were decrypted.
22	Compilation of the most important systems of the army, airforce and NKVD 1941/45 which were broken or captured.

23. Comparative table of alphabets.

24. Commitment of signal intelligence against the East.

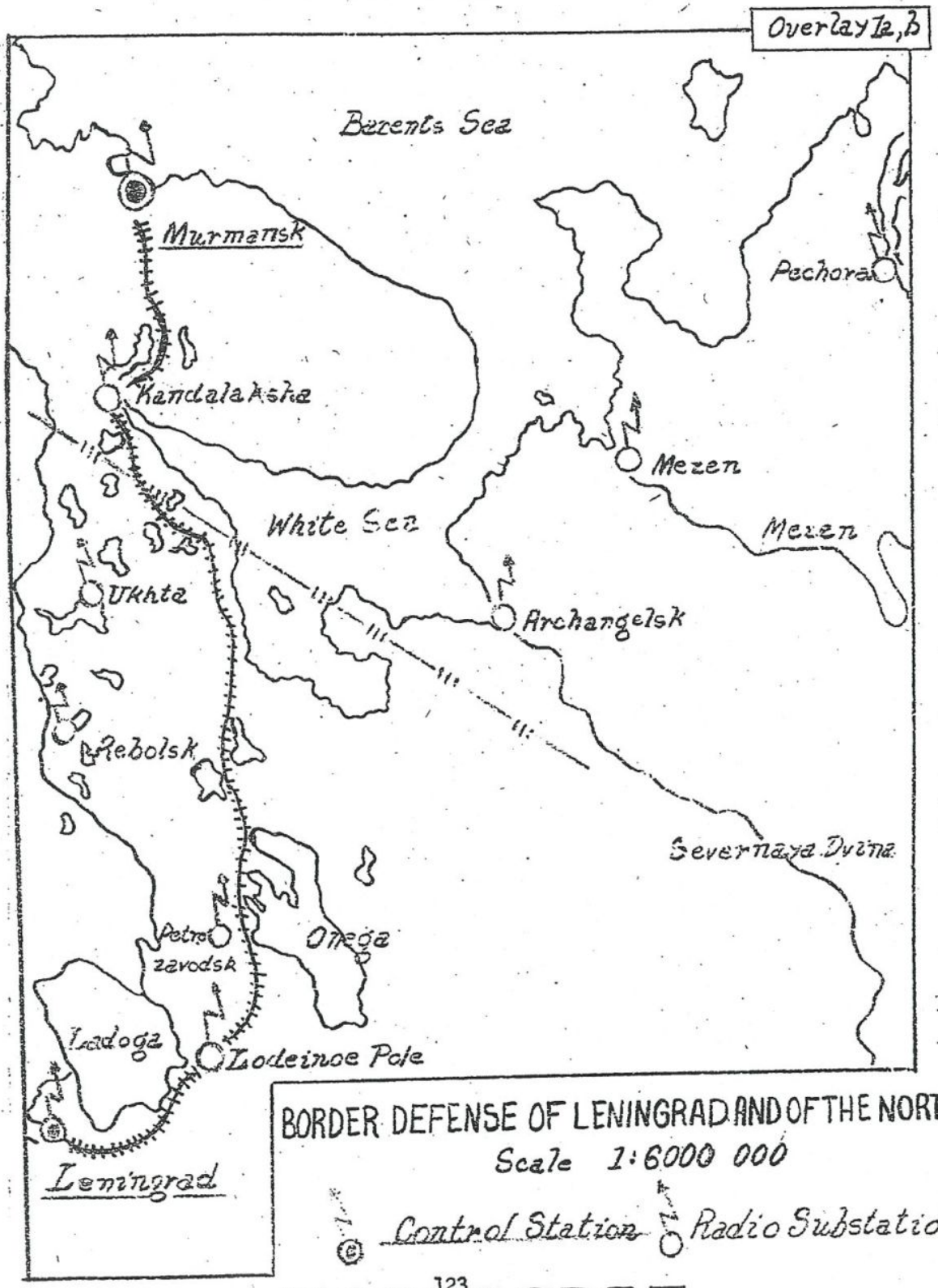
25 Table showing accomplishment and personnel strength of the fixed intercept station Jüterbog (Treuenbrietzen) with out-stations 1935--1939.

26 Comparison of personnel strength of the Russian section with accomplishments (1939--1945).

Supplement

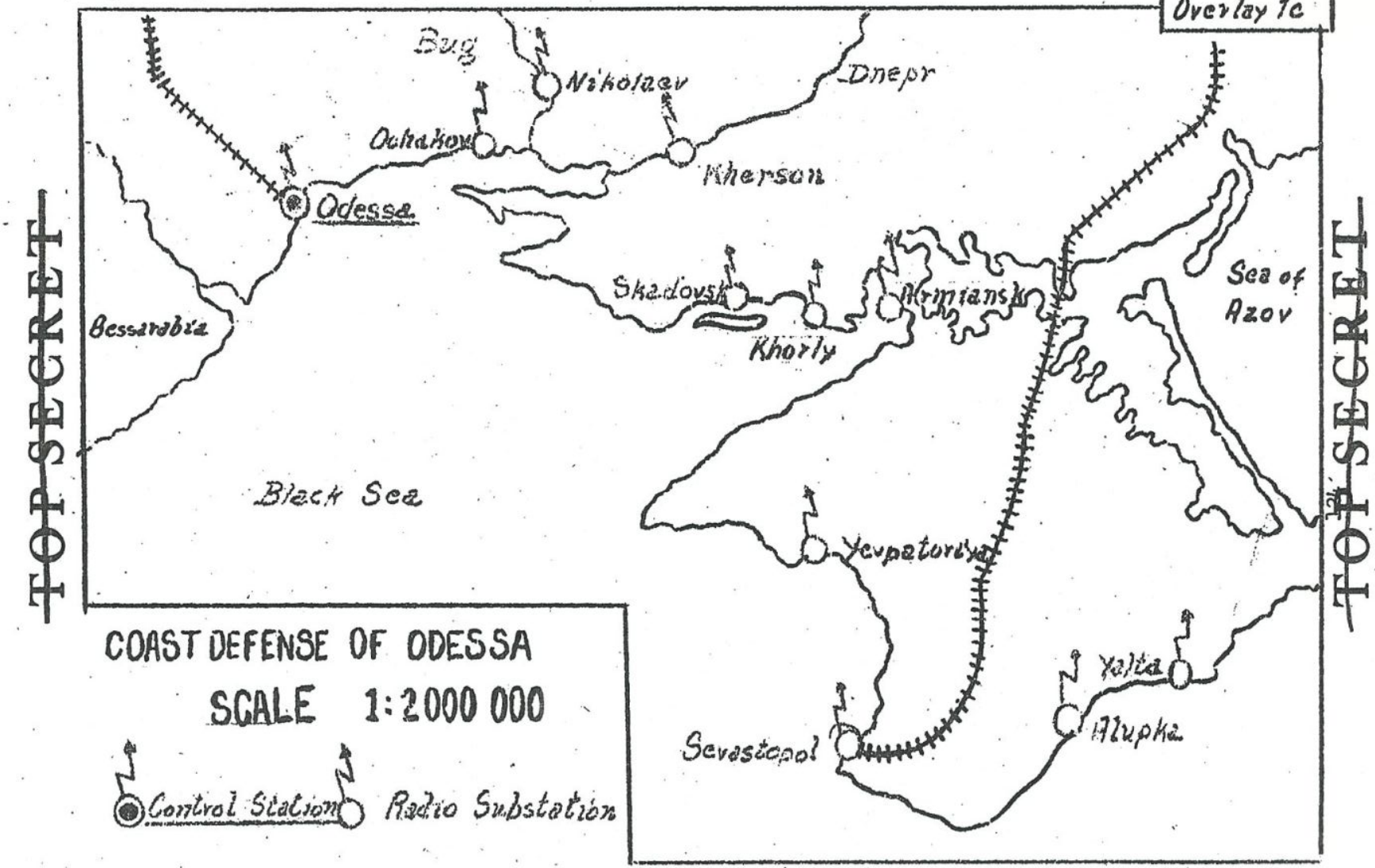
Cryptanalytic aids and methods particularly for Russian cryptograms. [outline only]

Problems of cryptanalysis
[outline, also text of Part II Section B]


Overlay Ia, b
Barents Sea
Murmansk
Pechora
Kandalaksha
Mezen
White Sea
Mezen
Ukhta
Archangelsk
Severnaya Dvina
Onega
Petrozavodsk
Ladoga
Lodeinoe Pole
Leningrad
BORDER DEFENSE OF LENINGRAD AND OF THE NORTH
Scale 1:6000 000
Control Station
Radio Substation

TOP SECRET

Overlay 1c



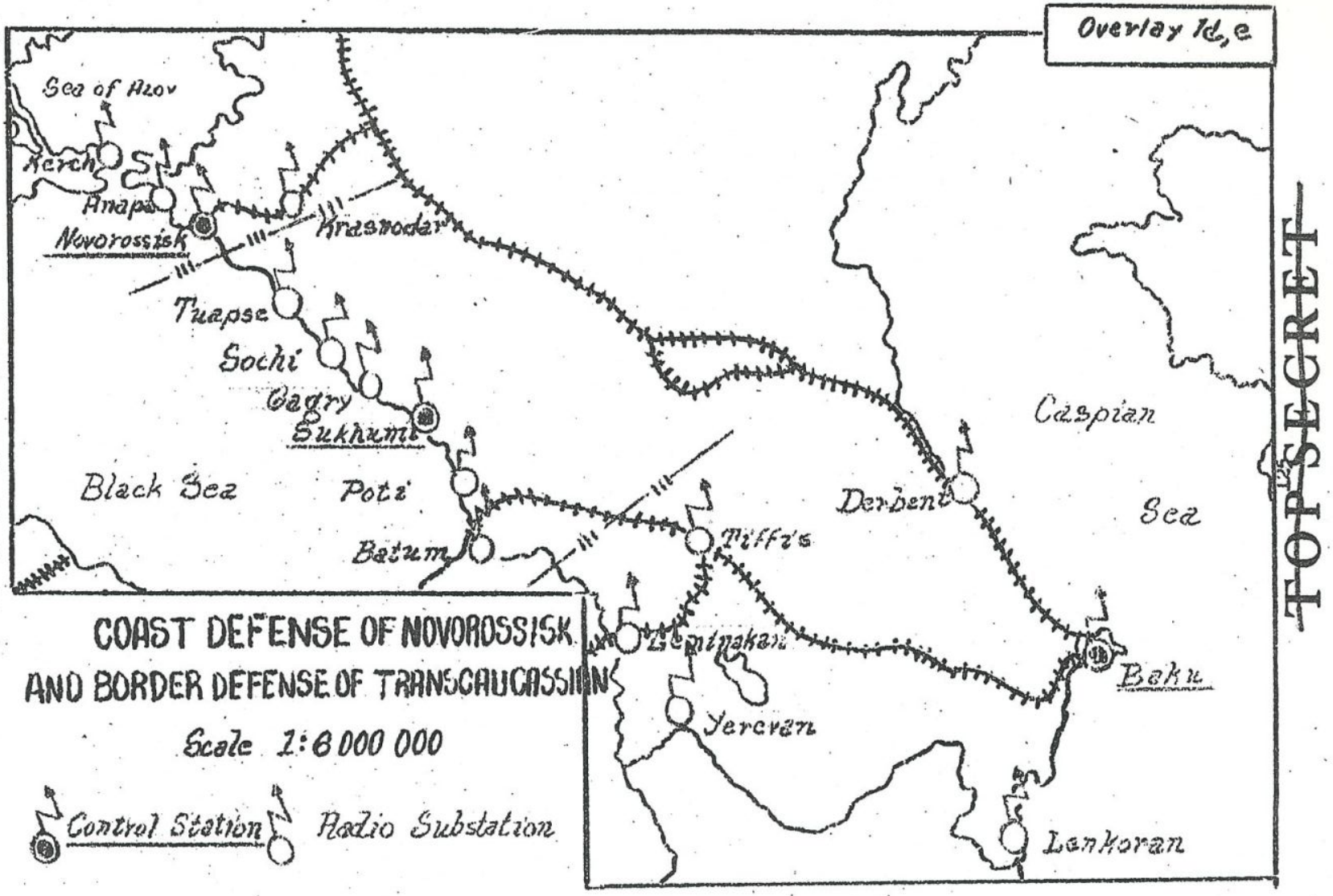
COAST DEFENSE OF ODESSA

SCALE 1:2000 000

Control Station Radio Substation

TOP SECRET

TOP SECRET

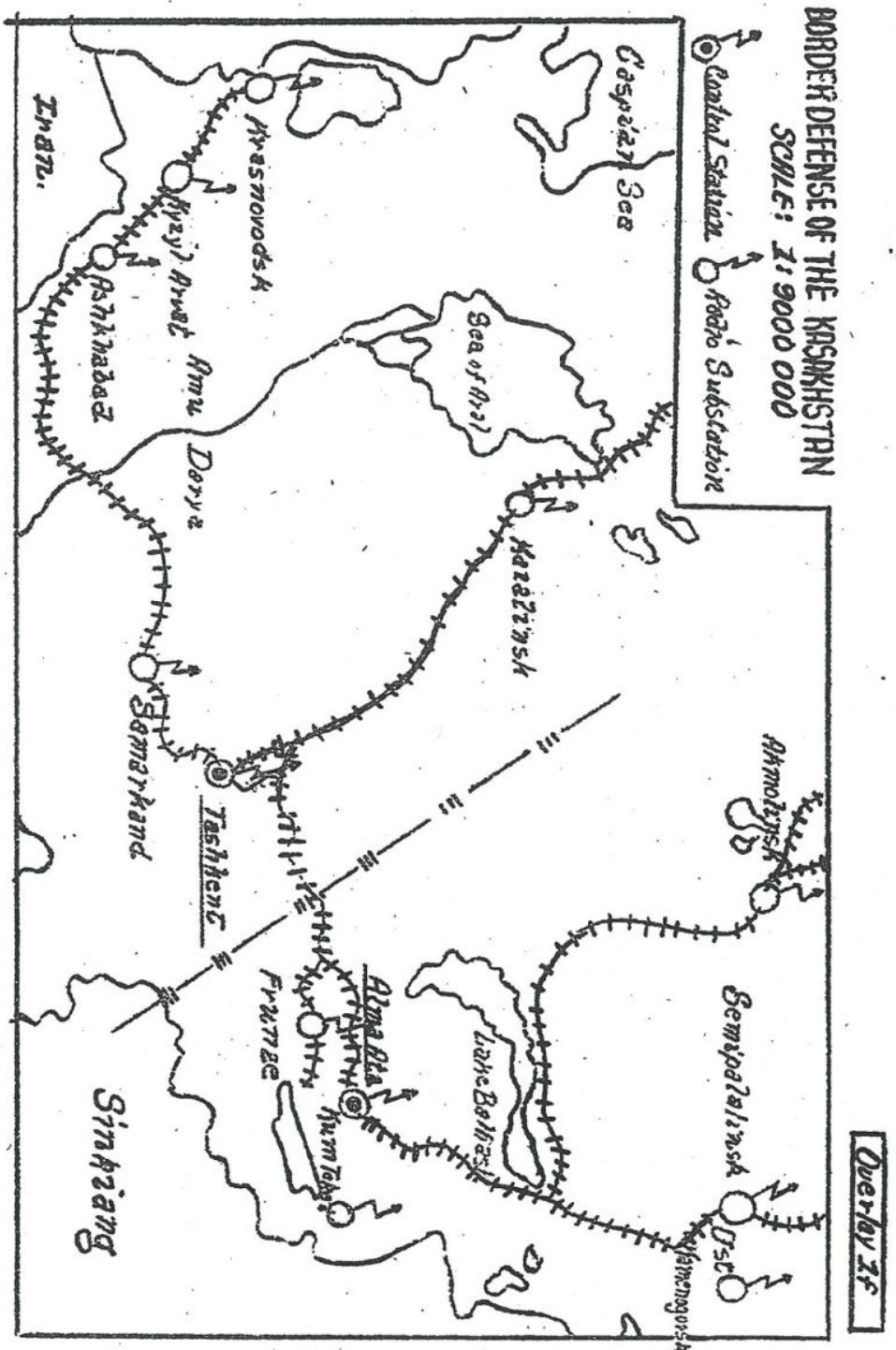


COAST DEFENSE OF NOVOROSSISK
AND BORDER DEFENSE OF TRANSCAUCASSIA

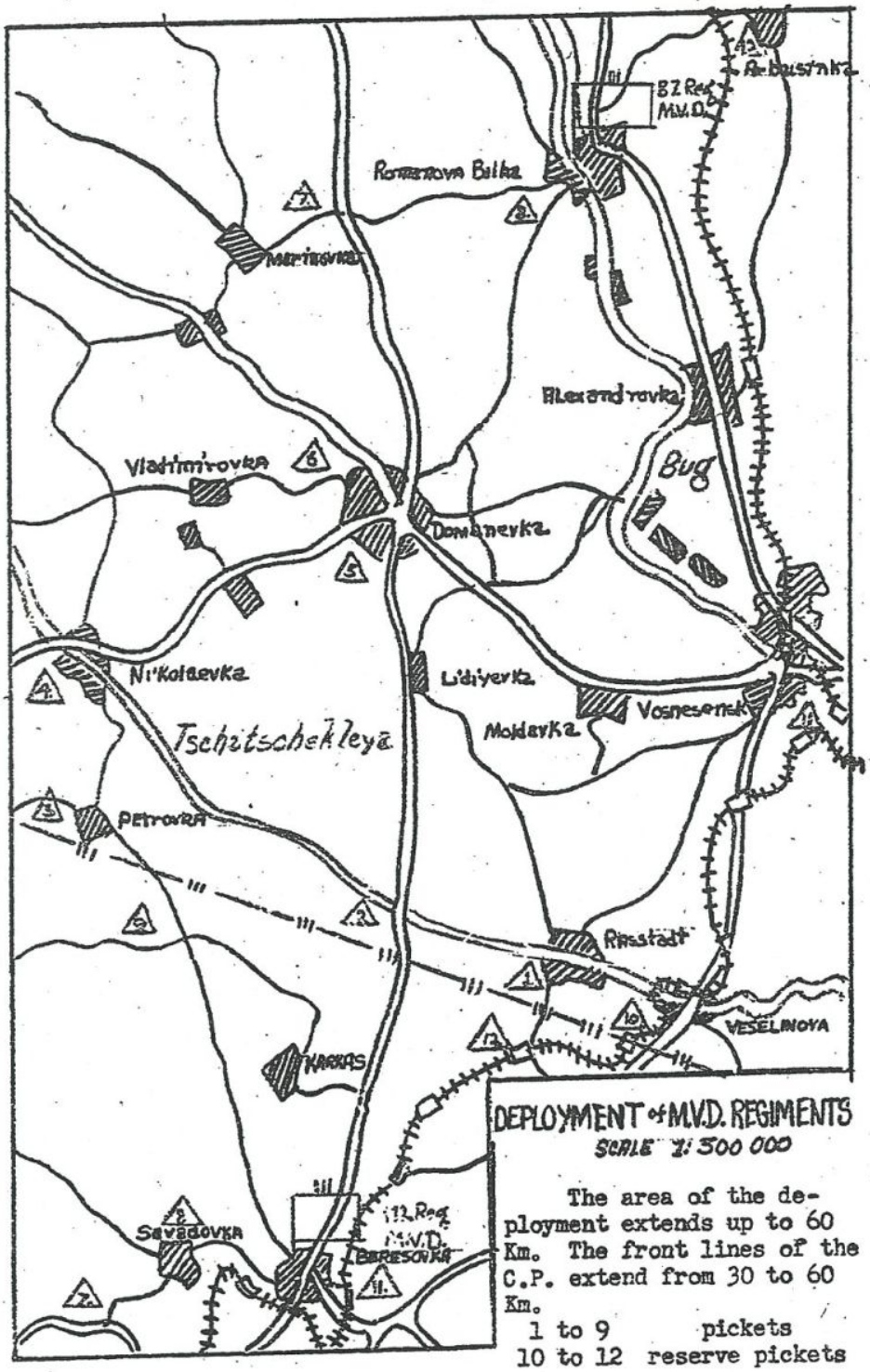
Scale 1:6 000 000

Control Station Radio Substation

TOP SECRET


BORDER DEFENSE OF THE KASAKHSTAN
SCALE: 1:9000 000
Control Station
Radio Substation
Caspian Sea
Sea of Aral
Krasnovodsk
Kyzyl Arvat
Ashkhabad
Amu Darya
Iran.
Kazalinsk
Samarkand
Tashkent
Akmolinsk
Semipalatinsk
Ust
Lake Balkhash
Alma Ata
Kum Tokai
Frunze
Sinkiang
Overlay 1f

~~TOP SECRET~~ Overlay 2



DEPLOYMENT of M.V.D. REGIMENTS
SCALE 1: 500 000

The area of the deployment extends up to 60 Km. The front lines of the C.P. extend from 30 to 60 Km.

1 to 9 pickets
10 to 12 reserve pickets

~~TOP SECRET~~

TOP SECRET

TABLE OF GENERAL TYPES OF CRYPTOGRAPHIC SYSTEMS ARRANGED WITH RESPECT TO SIZE AND TO USE

APPENDIX 3

Army and Airforce

Designation	Size (Number of groups)	General Staff	Front Staff	Army	Corps	Division	Brigade	Regiment	Battalion	Company	Platoon	Squadron	Remarks
Chiffre (5-digit)	10,000 - 25,000	+	+	+	+	+	+						-
Code (4-digit)	3,000 - 10,000			+	+	+	+	+					Not used since 1942
Code Table (4-digit)	2,000 - 3,000												Not in use.
SUV (3 & 4 digit)	500 - 2,000			+	+	+	+	+	+	+			-
PT (2,3 & 4 digit)	100 - 500							+	+	+	+	+	-

MKVD

Designation	Size (Number of groups)	GUF NKVD	Front Staff	Division	Brigade	Regiment	Agency	Battalion	Outposts	Oper. Group	Guard Group	Special Cmd.	Remarks
Chiffre (5-digit)	10,000 - 25,000												Predominently economic messages with 1 time additive.
Code (4-digit)	3,000 - 10,000	+	+	+	+	+	+						-
Code Table (4-digit)	2,000 - 3,000			+	+	+		+	+	+	+		-
SUV (3&4-digit)	500 - 2,000												Not in use.
PT (2,3 & 4-digit)	100 - 500					+	+	+	+	+	+	+	-

TOP SECRET

4.

TOP SECRET

	16			6				17	
		11				27			4
30			15		3		14		
7					1			10	
		20		26		19			
			9		24		12		
28		5							13
					18		29	21	
	8		25			2			
	31			23					22

7	8	3	2	6	0	5	4	9	1
8	4	5	0	2	9	6	1	3	7
5	6	1	4	3	7	9	0	2	8
0	1	6	7	4	8	2	9	5	3
3	9	7	5	8	4	1	6	0	2
4	3	2	9	5	1	0	7	8	6
9	2	0	1	7	3	4	8	6	5
6	0	8	3	9	2	7	5	1	4
1	5	4	8	0	6	3	2	7	9
2	7	9	6	1	5	8	3	4	0

А	К	ф	Э	0	ВОЛН	ОТВЕТ	ВАМ	ТОЧН	МЕТЕО
Б	Л	Х	1	(.)	ПОЗЫВН	ТЕЛЕГРАММ	ВАШ	СРОЧН	СВОДКА
В	М	Ц	2	(..)	РР.	ПРИЕМНИК	НАШ	СООБЩ	ВЕТЕР
Г	Н	Ч	3	(-)	РАДИО	ПЕРЕДАТЧ	НЕТ	ДОНЕСТИ	ЭСН
Д	О	Ш	4	(-.)	ПЛАН	МОЛНИЯ	КОГДА	СОГЛАСН	ПОЛК
Е	П	Щ	5	НР.	МЕТР.	ЧАС	КУДА	ДИРЕКТИВ	БАТ.
Ж	Р	Ы	6	НАЧ	КМ.	МИН.	КТО	ПРИКАЗ	РОТА
З	С	Ь	7	ком.	РАЦИЯ	АККУМУЛЯТ	МАШИНА	ТЕЛЕФОНО	ВЗВОД
И	Т	Э	8	ПОМ	СЕТЬ	ГОРЮЧ	ЖЕЛЕЗНЫЙ	ПРОШУ	ПЛОХ
Й	У	Ю	9	ЗАМ	СВЯЗЬ	ВЫЗОВ	УДАЛЕН	ПОГОДА	ХОРОШ

129

TOP SECRET

4a Appendix

Example showing use of the first general army and airforce operational system with keys for one month.

Original designation: "ПТ" — 35" = Chatter table of the year 1935.
(Russian 2-digit substitution)

The system squares serving for encipherment are so composed that all digits from 1—0 occur once in each row and column. The system square shown at the left above the basic substitution is ued to encipher both the tens and the units of the dinomes (cipher groups). In the upper left square are the 31 numbers corresponding to the day dates of a month.

Choice of key for the 9th of the month.

Below the day date 9 is the sequence: 2,0,4,7,5,9,1,3,8,6 = encipherment of the tens; on the line with the 9th, at the right, is the sequence 4,3,2,9,5,1,0,7,8,6 = encipherment of the units. The dihome formed from the first two digits of these sequences, here 24, is the indicator group for this encipherment.

Russian plaintext: ВАШ ПОЗЫВНОЙ - 4 ТЛ - ВОЛНА 173.
ЛИСИЦИН

Translation: Your call sign is — 4tl — wave 173

Cipher text with plaintext above (indicator for encipherment on the 9th).

Indicator	ВАШ	ПОЗЫВНОЙ	(—)	4	Т	Л	(—)
24	27	01	75	59	83	03	75

ВОЛНА	1	7	3	(·)	Л	И	С	И	Ц	И	Н
21	09	39	79	45	03	84	33	84	42	84	73

Or: 2427 0175 5983 9375 2109 3979 4503 8433 8442 8473 -

~~TOP SECRET~~

6	3	9	8	0	6	4	1	7	5	5.
А АВИА	К ВАШ	Ф ДАЛЕКО	9 ЗВЕНО	О МОЛНИЯ	ПЕЛЕНГ	РАБОТ	СООБЩ.			
Б АВТО	Л ВЗВОД	Х АВИАГИГАНТ	1 КЛЮЧ	(,) НАМ	П.Т.	РАДИО	СРОЧН.			
В АККУМУЛ.	М ВОЛН	Ц ДИРЕКТИВ	2 КОГДА	(.) НАС	ПЕРЕДАТЧ	РГ.	ТЕЛЕГРАФ			
Г АППАРАТ	Н ВЫЗОВ	Ч ДОНЕСТИ	3 КОМ.	(-) НАЧ.	ПЛОХ	РАДИСТ	ТЕЛЕФОН			
Д БАТ.	О ГДЕ	Ш ЕЖЕДНЕВН	4 КОНЕЦ	(/) НАШ	ПОДЫВН	РАЦИЯ	ЧИТАЙ БУКВЫ			
Е БЕЗ	П ГОРЮЧ	Щ ЕСЛИ	5 КТО	(?) НЕМЕДЛЕН	ПОГОДА	РОТА	УКАЗАНИЕ			
Ж БЕНЗИН	Р ГОТОВ	Ы ЕСТЬ	6 КУДА	(:) НЕТ	ПОЛК	СВЕРЯСЬ	УЧЕБН			
З БРИГАД	С ГОТОВНОСТ	Ь ЕЩЕ	7 МАТЕРИАЛ	НУЖН	ПОЧЕМУ	СВЯЗЬ	ХОРОШ			
И ВАМ	Т ГРУПП	Э ЗАМ	8 МАШИН	ОТБОЙ	ПРИЕМНИК	ЧИТАЙ СЛОВА	ЧЕРЕЗ			
Й ВАС	У ДАЙТЕ	Ю ЗАДАЧ	9 МЕСТО	ОТВЕТ	ПРОШУ	СОПАСН	ЧТО			

~~TOP SECRET~~

5a Appendix

Example showing use of the second general army and airforce operational system.

Original designation: "ПТ -39" = PT-39 = Chatter table of 1939 (Russian 2-digit substitution with double readings) [variants]

The two empty columns (20 cells), are for optional entries (different for each network.

Russian plaintext: КЛЮКОВУ.

ВАША РАДИОГРАММА НЕ РАСКОДИРУЕТСЯ, КАКИЕ КЛЮЧИ?

МУХИН

Translation: To Kljukov
Your radiogram cannot be deciphered,
What key? Muchin

Cipher text with plaintext above:

ЧИТАЙ БУКВЫ				К	Л	Ю	К	О	В	У	(.)			
01				63	33	29	63	03	42	23	40			
ЧИТАЙ СЛОВА		ВАША		РГ.		ЧИТАЙ БУКВЫ		Н	Е	Р	А			
54		63		44		01		73	92	13	62			
С	К	О	Д	И	Р	У	Е	Т	С	Я	(з)	К		
83	63	03	02	52	13	23	92	53	83	68	30	63		
А	К	И	Е	ЧИТАЙ СЛОВА		КЛЮЧИ		ЧИТАЙ БУКВЫ						
62	63	52	92	54		38		01						
(?)		М	У	Х	И	Н								
90		43	23	39	52	73								

Note: The underscored groups are switch groups, indicating in the one case "read letters" in the other case "read words". The cipher text may be transmitted in two or four digit groups.

TOP SECRET

6

	4	1	9	8	0	7	3	2	6	5
6	В ЗАДАЧ	1 КТО	И РАДИО	О ПЕРЕМЕН	Н НАХОД	Ч РАДИСТ	К СООБЩ.	2 КОМ	А ХОРОШ	Ц КОД
3	Р НАМ	6 ТЕЛЕГРАФ	Б УАС	Т ЕСТЬ	Ы КИЛОМЕТР	П ГДЕ	2 ПЕЛЕНГ	Ж АККУМУЛЯТ	Ф ВАМ	Е РАБОТ
2	Й РАЗВЕДК	Ж ОТБОЙ	Ф ЧТО	ЧИТАЙ БУКВЫ	О ГРУПП	В БАТАЛЬОН	С ПОМ.	(.) СМЕНА	Ы ПЕРЕДАТЧ	О МОЛНИЯ
8	7 ПРЕДСТАВ	Ч ЗАМ.	(-) РАЙОН	Л КУДА	Ю ГОТОВ	И НАЧ	Ц ВАШ	Г ПРИЕМНИК	Н КОНЕЦ	4 ДИРЕКТИВ
5	Л ЧЕРЕЗ	« ВСЕ	А РАДИОГРАМ	Щ ЕЖЕДНЕВН	1 НАШ	Н КУДА	8 ПОЛИТ	У БЕНЗИН	7 МАШИН	К ВОЛНА
0	(,) РЕЗУЛЬТАТ	П НЕМЕДЛ	(?) САМОЛЕТ	Х ПОГОДА	Д АППАРАТ	(.) ТОЧН.	Е ПЕРИОД	С МЕСЯЦ	Р ОТДЕЛ	Ш ПРОШУ
7	Е СРОЧН.	Н ГОРЮЧ	Ш СОСТАВ	С РАЦИЯ	В ДВИГАТЕЛЬ	З ЗАЧЕМ	Ь ВЗВОД	Я РОТА	А ДЛЯ	9 ПРИКАЗ
1	У ПОЗЫВН	О УЧЕБН.	(-) АВТО	» КЛЮЧ	Т ПЛОХО	5 ЧАСТ.	3 ПРИЕМ	М ПРОТИВНИК	ЧИТАЙ СЛОВА	Т СВЯЗЬ
9	Ю ВЫЗОВ	Г ДАНН.	В МИНУТ	9 ТАБЛИЦ	Ш МЕСТО	М ФРОНТ	5 ОТВЕТ	О ВАС	(,) КОГДА	Э ТЕЛЕФОН
4	3 МЕТР.	И ЛИНИЯ	6 СВОДКА	Д ПОЛК	Ь ШИФР	Х БЕЗ	Р ШТАБ	Я НАС	Й АВИА	З СЕТЬ

TOP SECRET

Appendix 6a

Example showing use of the last general operational system and emergency key of the army and airforce.

Original designation: "ПТ = 41" = PT = 41 – Chatter table of 1941

(Russian 2-digit substitution with variants)

Encipherment is still by stem squares and is sometimes changed several times a day within one network.

Russian plaintext: НАЧ. СВЯЗИ.
НАШ ПРИЕМНИК ОТКАЗАЛ, ДАЙТЕ ПО ТЕЛЕГРАФУ
РОТЭРМЕЛЬ

Translation: To Chief Signal Officer
Our receiver has gone bad, request transmission by telegraph.
Rotärmel

Cipher text with plaintext above:

ЧИТАЙТЕ СЛОВА	НАЧ.	СВЯЗИ	ЧИТАЙТЕ БУКВЫ	(.)	ЧИТАЙТЕ СЛОВА
16	87	15	28	22	16

НАШ	ПРИЕМНИК	ЧИТАЙТЕ БУКВЫ	О	Т	К	А	З	А
50	82	28	20	10	55	59	45	76

Л	(,)	Д	А	Й	Т	Е	П	О	ЧИТАЙТЕ СЛОВА
54	04	48	76	46	38	35	01	92	16

ТЕЛЕГРАФ	ЧИТАЙТЕ БУКВЫ	Р	О	Т	Э	Р	М	Е	Л	Ь
31	28	34	25	10	95	06	97	35	88	40–

Note: Underscored groups are switched groups reading "read letters" and "read words".

TOP SECRET

TOP SECRET

7.

	А	Н	ф	Е	С	Р	Ч	Л	Ь	Щ
8	О		А	Б	У	ф	Х			
3		1	В	Г	Ц	Ч	Ш			
9			2	Д	Щ	Ы	Ь			
1			Е	З	Э	Ю	Я			
6			Ж	З	4	Й				
4			И	К		5				
5			Л	М		(.)	6			
0			Н	О		(-)		7		
7			П	Р		НОМЕР			8	
2			С	Т						9

Appendix 7a

Example showing use of the substitution system of the border guard districts North, Leningrad, Kasakstan.

Original designation unknown (Russian digit — letter — substitution).

Encipherment by the aid of a letter square and a digit square. Change encipherment daily.

Since border guard districts North and Leningrad had no other systems down to 1938 this was also used as a general system.

The blankscells were filled gradually with operational and technical words and expressions, these differed with the three networks.

Russian text:

КОМ. ДИВ. ПРИБЫЛ

ПРИВЕТ БОГОМОЛОВУ.

Translation: The section chief has arrived.
Greetings to Bogomolov.

Cipher text with plaintext above.

К	О	М	(·)	Д	И	В	(·)	П	Р	И
4Е	0Е	5Е	5Р	9Е	4Ф	3Ф	5Р	7Ф	7Е	4Ф

Б	Ы	Л	П	Р	И	В	Е	Т	Б	О
8Е	9Р	5Ф	7Ф	7Е	4Ф	3Ф	1Ф	2Е	8Е	0Е

Г	О	М	О	Л	О	В	У	(·)	
3Е	0Е	5Е	0Е	5Ф	0Е	3Ф	8С	5Р	–

TOP SECRET

8.

	7	0	3	9	6	8	1	5	2	4
4	0	1	2	3	4	5	6	7	8	9
8	НАЧ	КОМ	ЗАМ	ПОМ	УПВО	НКВД	ОТДЕЛ	ОТРЯД	ЗАСТАВ	ПОСТ
5	А	Б	В	Г	Д	Е	Ж	З	И	Й
1	АККУМУЛ	АППАРАТ	БАЗА	БЕЗ	ВОЛНА	ВРЕМЯ	ВЫЗОВ	ГОТОВ	ГРУППА	ДАЙТЕ
6	ДАННЫ	ДЛЯ	ДОНЕСИТЕ	ЕЖЕДНЕВН	ЕСЛИ	ЕСТЬ	ЖДУ	ЗАДАЧУ		
3	К	Л	М	Н	О	П	Р	С	Т	У
0	КЛЮЧ	МЕСТО	МЕТР.	МИНУТ	ОТВЕТ	ПОЗЫВН	РАБОТ	РАДИО	РАДИСТ	РГ
7	РАЦИЯ	СВЯЗЬ	СЕТЬ	СООБЩ	СРОЧНО	ТОЧН.				
2	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю
9	Я	(.)	(,)	(-)	(/)	НОМЕР	ХОРОШ	ЧАС		

137

TOP SECRET

Example 8a

Example showing use of the substitution system of the coast guard district Novorossisk.

Encipherment by use of a system square. Change of key approximately every week.

Since no other systems were available in the coast guard district Novorossisk down to 1938 this was also used as a general system.

Russian plaintext:

НАЧ. ОТДЕЛА УПВО НКВД(.)
ПРОШУ СООБЩИТЬ НОВЫЕ РАДИОДАННЫЕ НА ФЕВРАЛЬ.
НАЧ. 3. ОТРЯДА ГОРКОВЕНКО

Translation: To section leader UPVO NKVD.
Please send keys of February
Leader of the 3rd sub-section Gorkovenko

Cipher text with plaintext above:

НАЧ.	ОТДЕЛА	УПВО	НКВД	(.)	П	Р	О	Ш	У	СООБЩИТЬ
87	81	86	88	90	38	31	36	26	34	79

Н	О	В	Ы	Е	РАДИО	ДАННЫЕ	Н	А	Ф	Е	В	Р	А
39	36	53	21	58	05	67	39	57	27	58	53	31	57

Л	Ь	(.)	НАЧ.	З.	ОТРЯДА	Г	О	Р	К	О	В	Е	Н	К	О
30	25	90	87	49	85	59	36	31	37	36	53	58	39	37	36

Note: The cipher text is sent in 6-digit groups, the final group is padded with random digits when necessary.

0	1	2	3	4	5	6	7	8	9
КОМ.	НАЧ	ЗАМ.	ПОЛ.						
ВЗВОД	ГРУППА	ЗАСТАВ	ЗВЕНО	ОТДЕЛ	ОТРЯД	ПОСТ	ЧАСТ	УПВО	НКВД
А	Б	1	В	2	Г	Д	Е	З	Ж
3	4	И	Й	К	Л	М	Н	О	П
7	О	П	Р	С	Т	У	Ф	Х	Ц
Ф	Х	Ц	Ч	Ш	Щ	Ы	Ъ	Э	Ю
9	(.)	(,)	(-)	НОМЕР	(/)				
ПЛАНШЕТ	БЕЗ	ВОЙНА	ВРЕМЯ	ГОТОВ	ДАННН	ДОЛЖ	ДОНЕСТН	ЕЖЕДНЕВН	ЗВОНОЧ
КЛЮЧ	КМ	МЕСТО	МЕТР	МИНУТ	ОТВЕТ	ПОЗЫВН	РАБОТ	РАЗНО	РЕГ
РАЦИЯ	СВЯЗЬ	СООБЩ	СРОЧН	ЧАС					

Appendix 9a

Example showing use of the substitution system of the coast guard district Odessa.

Original designation unknown (Russian 2-digit substitution with nulls).

Encipherment by use of a system square. Change of key about every week.

In the cipher text a null is inserted between the first and second, third and fourth, fifth and sixth, ... etc. groups. Thus null increases progressively by one. The groups in the cipher text are therefore 5-digit, the middle digit being the null.

Russian plaintext:

ВСЕМ НАЧ. ЗАСТАВ.
СРОЧНО УСИЛИТЬ ОХРАНУ БЕРЕГА.
НАЧ. ОТДЕЛА УПВО НКВД

Translation: To all leaders of (coast) outposts.
Reenforce the coast patrol at once.
Section leader UPVO NKVD

Cipher text (intermediate text) with plaintext above:

ВСЕМ	НАЧ.	ЗАСТАВ	(.)
64 52 60 39	03	71	43

СРОЧНО	УСИЛИТЬОХРАНУ	
14	59 52 31 35 31 50 90 53 93 57 68 36 59	

БЕРЕГА(.)	НАЧ.	ОТДЕЛА	УПВО	НКВД
63 60 57 60 62 68 43	03	77	79	76

Cipher text divided into groups with nulls underscored:

64452 60539 03671 43714 59852 31935

31050 90153 93257 68336 59463 60557

60662 66713 03877 79976 -

4	1	0	6	3	0	8	5	2	7	10.
О	ВАМ	А	ВАШ	Б	ВАС	В	ГО	Г	ГДЕ	
НАМ	1	ВСЕ	Д	Д,О	Е	КО	Ж	ЗА	З	
И	ИЗ	2	ДЛЯ	Й	НА	К	КОМ	Л	ЗАМ	
НАС	М	НАШ	З	НЕ	Н	НАЧ	О	ОТ	П	
Р	ПО	С	СВЯЗЬ	4	НКВД	Т	НО	У	ПОМ	
РГ	Ф	УПВО	Х	ДИВ	5	ПРИ	Ц	ПРО	Ч	
Ш	ШТАБ	Щ	ПОЛИТ	Ы	ПОСТ	Э	ЧТО	Ь	ЭШЕЛ	
ПРЕД	Э	ОТДЕЛ	Ю	ПОГРАН	9	ОТРЯД	7	ЧАСТ	НОМЕР	
(,)	(/)	(.)	(:)	(-)	(?)	МЕТР	ПОЗЫВН	8	ВОЛН	
СРОЧН	КМ	ВЫЗОВ	ЧАС	КУДА	МИНУТ	ОТВЕТ	СООБЩ	КОГДА	0	

Appendix 10a

Example showing use of the substitution systems of the border guard Transcaucasus.

Original designation unknown.
(Russian expanded 2-digit substitution with transposition)

Encipherment is with the aid of a system square. Change of key approximately once a week.

Plaintext is first converted into cipher text. This cipher text is treated as an intermediate text and divided up into sections of 5-cipher groups each. Within these sections the tens of the 5-cipher groups are combined into a 5-digit group, then the units are combined in like manner. The individual sections are separated from one another by bars and may be transposed at will.

Russian text:

НАЧ. ОТРЯДА ГАГРИ.

СРОЧНО СООБЩИТЕ ГДЕ НАШ П.К. 7. УПВО НКВД КАКАБАДЗЕ.

Translation: To the leader of the Subsection (in) Gagri.
Report at once location of our steam cutter 7.
UPVO NKVD Kakabadse.

Intermediate text with plaintext above.

I.

НАЧ.	ОТРЯДА		Г	А	Г	Р	И	(•)	СРОЧНО	СООБЩИТЕ	ГДЕ
18	28		82	89	82	44	64	79	34	35	87

НАШ	П	(•)	К	(•)	7	(•)	УПВО	НКВД	К	А	К	А	Б	А
19	17	79	68	79	25	79	09	40	68	89	68	89	83	89

Д	З	Е	(•)
56	57	50	79

II. 12888 88292 - 46733 44945 - 81176 79798 -

72704 95990 - 68688 89893 - 85557 96709 -

Cipher text:

81176 79798 - 85557 96709 - 46733 44945 -

68688 89893 - 72704 95990 - 12888 88292 -

TOP SECRET

	↓	47	63	05	19	28
7	2-6	1	НЕМЕЦК	НАСТУПЛЕНИЕ	ТАНК,ов	ТУМАН
	7-1	НЕМ,ецкий	НАСТУПАТЬ	НАХОД.	ТРОФЕЙ	ТОЧКА(.)
6	1-5	НАЧ	2	НАЧАЛО	ТИРЕ(-)	Т
	6-0	НОМЕР	Н	ДИВИЗИЯ	ЧАСТ,ей	ЧАС,ов
9	8-2	ХОРОШ	Х	3	ЧЕЛОВЕК	Ч
	3-7	ВОСТОК	ВЫХОД	ВЗАИМОДЕЙСТВ	ВЕСТИ	ВЕДУТ
8	5-9	ВОСТОЧН	ВОЕН.	ВОЕННН.	4	ВХОД
	0-4	ВЗЯТЬ	ВБЛ, а/м/ь	ВОКЗАЛ	Д	ДОРОГ
5	4-8	ВЗЯТО	В	САНИТАРН.	ЭСН, о	5
	9-3	СОСТАВ	СООБЩ.	СЕВ.ВОСТОК	СЕВ.ВОСТОЧН	СГОРЕЛ
0	8-2	СИЛ	СОГЛАСН	СЕВ.ЗАПАД	СЕВ.ЗАПАДН	СГОРЕТЬ
	3-7	СЕВЕР	СЕВЕРН.	СТАНЦИ,ей	СТРЕЛКОВ	СНАЙПЕР
3	1-8	СЕРЖАНТ	СТАРШИН.	САМОЛЕТ	С	А
	9-3	ГОРОД	ГЕФРЕЙТОР	АРМИ.	АВИАЦИ.	АРТИЛЛЕРН.
1	2-6	ГОРЮЧ	Г	З	И	Й
	7-1	ГСМ	РАЗВЕДК.	ЗАКРЕПИТЬ	ЗАКРЕПЛЕН	ЗАПАД
4	6-0	ГОТОВ	ГЕНЕРАЛ	ЗАПАДН.	ЗОН.	91
	1-5	ГОТОВНОСТ	РАЗРУШ	ЗПТ.(,)	ЗАМ.	ДЕРЕВН.
2	0-4	ГРУПП	РЕКА	РУБЕЖ	РАЙОН	РЕЗУЛЬТАТ
	5-9	ГРАНАТ.	РУЖЕЙН.	РОТА	Р	00
		81	40	23	67	59

96	72	14	30	85	↓	
ПОЛ,ов,я	ПОЛКОВНИК	ПОДПОЛКОВНИК	ОЗЕРО	ОТХОД	7-1	4
ПОЛК	ПРОТИВНИК	ПУЛЕМЕТ	ОГОНЬ	ОРУДИЕ	2-6	
ПОМОЩЬ	ПУНКТ	ПУЛЕМЕТН.	ОБЕСПЕЧ	ОКРУЖЕНИЕ	0-4	1
ПЕХОТА	ПТО	ПОМ.	ОБХОД	ОБСТРЕЛ	5-9	
ПЛЕН	ПОСЛЕ	ПОТЕР.	О	ФРОНТ	6-0	0
ПЛЕННН.	П	ЖЕЛ.ДОРОГ.	ЖЕЛ.ДОРОЖН	ЖЕРТВ	1-5	
УДАЧН.	УНИЧТОЖ	УЛИЦ	УБИТ	УЧАСТОК	9-3	2
УДАР	УДАЛОСЬ	К	У	Е	4-8	
КОММУНИКАЦ	КП	КАПИТАН	БЕЗ	БОЙ	3-7	3
КОНТР.	КМ	КАВАЛЛЕРИ	БАТАЛЬОН	БОЛОТА	8-2	
В	КОРПУС	КУРС	БРИГАД	БАНД.	4-8	9
КУДА	КОГДА	КТО	В	БОЛЬШ.	9-3	
КОЛИЧЕСТВ	7	КРАСНОАРМЕЕ	БОМБОМЕТЧИ	Э,Ъ	8-2	7
КОМ.	М	ЮЖН.	ЮГ	ЮГО-ВОСТОК	3-7	
МАЙОР	МЕТР.	В	ЮГО-ЗАПАДН	ЮГО-ВОСТОЧН	7-1	5
МИНОМЕТ	Ж,Ц	ЮГО-ЗАПАД	Ю	Ш	2-6	
МИНОМЕТН	МОТОР	МИНУТ	Э	ЩТАБ	5-9	6
МАРШРУТ	МАРШ	МЕЛК	МЕЖД.	Щ	0-4	
МАШИН	МАТЕРИАЛ	Л	Ь,Ы	О	1-5	8
ООО	МОСТ	ЛИНИЯ	ЛЕЙТЕНАНТ	ЛЕС	6-0	
07	35	98	64	21		

TOP SECRET

Appendix 11a

Example showing the use of a small tank signal table "SUV" system.

Russian 4-digit code.

The tank signal table with 200 groups shows an interrupted, partially alphabetic sequence, i. e. the words with the same initial letter are grouped together with a few exceptions. Aside from the most important words for tank warfare the code contains 1-digit numbers, the most important marks of punctuation and an auxiliary alphabet where some letters are used selectively corresponding to the text.

Encipherment is by dinomial substitution for elements AB and single digit substitution for elements C and D. It is changed at the discretion of the signal officer concerned. Each code value may be expressed in 5 different ways in respect to the cipher element D.

Manner of reading the group is in the sequence: column (dinome in the upper or lower margin of the table) — double row (single digit at the left and right outer margin of the table) — row (single digit at the left and right inner margin of the table, this may be expressed in five ways).

Russian plaintext:

ПРОТИВНИК СИЛОЮ ДО 1 БАТАЛЬОНА И ТАНКИ В РАЙОНЕ 27439, 27447, 27448, 28433 И 28441, ОБХОД С СЕВЕРА УДАЛОСЬ КАПИТАН РУДИН

Translation: Enemy and strength of one battalion and tank (is) in the area 27439, 27447, 27448, 28433 and 28441, encirclement of Norden has succeeded.
Captain Rudin.

Cipher text with plaintext above:
(Insignificant words and 5-digit coordinates are not enciphered).

ПРОТИВНИК	СИЛОЮ	ДО	1	БАТАЛЬОНА	И	
7245	8100	ДО	4775		3032	И

ТАНКИ	В	РАЙОНЕ	27439	27447	27448	28433
1973	В	6723	27439	27447	27448	28433

И	28441	ОБХОД	С	СЕВЕРА	УДАЛОСЬ	(.)
И	28441	3019	С	8105	7227	2877

КАПИТАН	Р	У	Д	И	Н
1436	6726	3023	1[illegible]4	4715	6369

12.(a).

		37, 52 84, 90	04, 29 41, 63	18, 35 57, 72	00, 26 46, 92	13, 52 51, 86	11, 20 66, 98	03, 14 33, 89	22, 28 47, 69	17, 34, 56, 75	08, 48 55, 79	
0	0	А	АВАРИЯ							УБИТ		
	1	Б				ИСТРЕБИТЕЛЬ			РАБОТ			
	2	БЕЗ	АВИА									
	3	В	АВИАЦИЯ						РАДИО			
	4	ВАМ			ДЕЖУРН.		НАБЛЮДЕН		РАДИОТЕЛЕФОН		БЕЛОВ	
	5	ВАС						ОЧЕНЬ		УНИЧТОЖ		
	6	ВАШ							РАДИСТ			
	7	ВЫ	АВТО									
	8	Г	АВТОМОБИЛИ		ДЕРЕВНЯ							
	9	ПО										
1	0	Д								ФАКТ		
	1	ДА		ВОЗДУХ	ДЕСАНТ		НАЛЕТ	ПАРК				
	2	ДО		ВОЗДУШН.					РАЗРЕШ.			
	3	Е				КАРТА						
	4	Ж	АВТОМОБИЛЬТОР				НАМ		РАЗРУШ		ГАГРИН	
	5	З						ПАРТИЯ				
	6	ЗА		ВОЛНА					РАЙОН			
	7	Ж								ТОРОШ		
	8	ИЗ			ДИВИЗИЯ						ДУХОВСКИЙ	
	9	К	АППАРАТ									
2	0	КО					НАС				ЕРМОЛОВ	
	1	Л			ДИРЕКТИВ	КОГДА		ПЕЛИГ				
	2	ЛИ							РЕКА	ЦЕЛЬ		
	3	М	АЭРОДРОМ								ЗАКЕНКО	
	4	Н	АЭРОПОРТ				НАХОДИТ					
	5	НА				КОМАНДИР		ПЕРЕЛЕТ		ЧАСТЬ		
	6	НЕ		ВОСТОК			НАЧАЛЬНИК					
	7	НИ		ВОСТОЧН								
	8	НО				КОММИССАР			РОТА			
	9	О	БАЗА				НАШ	ПОЗЕМЛЕНИЕ		ЧЕЛОВЕК		
3	0	ОБ										
	1	П			ДОЖДЬ			ПОЗЫЕН		ЧЕРЕЗ		
	2	ПЕ		ВРЕМЯ				ПОЛЕТ	РУБЕЖ			
	3	ПЕРЕ	БЕНЗИН					ПОЛИТ				
	4	ПО		ВСЕ	ДОНЕСТИ					ЧТО		
	5	ПРЕД	БЕРЕГ		ДОНОШУ		НЕМЕДЛЕН		САМОЛЕТ		ЛЮБОВ	
	6	ПРИ				КТО		ПОСАДКА				
	7	ПРО			ДОПОЛН	КУДА						
	8	Р						ПОЧЕМУ		ШТАБ		
	9	РАЗ	БЛАГОДАРЯ									
4	0	О		ВЫЗОВ	ДОРОГА				СГОРЕЛ		МИЛАДЗЕ	
	1	СО	БОЛЬШ			КУРС						
	2	Т	БОМБ			КУРСАНТ						
	3	ТЕ	БОМБАРДИРОВ	ВЫЛЕТ								
	4	ТО			ДРУГ			ПРИБЫЛ		ШТУРМ		
	5	У	БОМБИТЬ			ХУЧЕВ		ПРИБЫТИЕ		ШТУРМАН		
	6	Ф			ДЫМКА		НОРМАЛЬН		СЕВЕР	ШТУРМОВИК		
	7	Х		ВЫСОТА				ПРИЕМ	СЕВЕРН			
	8	Ц					ПОЧЬ					
	9	Ч		ВЫСЛАТЬ								

Ø

1

2

3

4

12.(b)

5	0	Ш	БОРТ		ЕСЛМ	ЛАГЕРЬ	НУЖН	ПРИЛЕТ	СЕЛ	ЭКИПАЖ	НИКИТИН
	1	Щ			ЕСТЬ						
	2	Ы									
	3	Ь			ЕЩЕ			ПРИЧИН	СЕТЬ	ЭСКАДР	
	4	Э									
	5	Ю		ГАРНИЗОН		ЛЕС					
	6	Я				ЛЕТ					
	7	(.) ЗПТ.	БРИГАДА			ЛЕТНАБ		ПРОИЗВЕЛ		ЭШЕЛОН	
	8	(.) ТУХ.				ЛЕТЧИК		ПРОИЗВЕСТИ			
	9	(.) ТИРЕ									
6	0	(.) ЖЕТЧК		ТДЕ	ЖЕРТВ		ОБЕСПЕЧ		СНЕГ	ЮГ	
	1	НОМЕР				ЛУЧШЕ	ОБЛАЧНОСТЬ				
	2	ЧАС					ОБНАРУЖ		СООБЩ	ЮЖН.	
	3	МИНУТ			ЗАМЕСТИЛЬ	ЛЫЖ		ПРЛЕТ			
	4	МЕТР.	БЫЛ								
	5	КИЛОМЕТР	БЫТЬ		ЗАПАД		ОД				
	6	МИНУС		ГОДЕН	ЗАПАДН				СООТАВ		РУЖИН
	7	ПЛЮС									
	8	ВЕРСТ									
	9	АРШИН									
7	0	000	ВАЖН.		ЗВЕНО	МАРШ	ОЖИДАЮ		СРОЧНО	ЯСНО	
	1	00		ГОРОД		МАРШРУТ					
	2	0			ЗЕНИТН	МАСЛО	ОЗЕРО		СТАРТ		
	3	1		ГОРОД				ПРОПУСК	СТАРТ		
	4	2				МАТЕРИАЛ					
	5	3						ПРОПУСК			
	6	4		ГОТОВ		МАШИН					СТЕПАНОВ
	7	5		ГОТОВНОСТ							
	8	6			ЗОНА.		ОРУЖИЕ				
	9	7									
8	0	8	ВЕЛ			МЕСТО		ПРОТИВНИК	ТЕЛЕГРАФ	-Р-5-	
	1	9		ГРУЗОИК							
	2	10					ОСТАЛЬН				
	3	20		ГРУППА		МЕТЕО		ПРОШЛО			
	4	30				МЕТЕОСВОДК		ПРОШУ	ТОЛЬКО	-Н-15-	
	5	40					ОТБОЙ				
	6	50									
	7	60	ВЕТЕР				ОТДЕЛ		ТОЧН.		
	8	70				МОЛНИЯ					
	9	80								-СБ-	
9	0	90	ВЗЛЕТ		ИНЖЕНЕР			ПУЛЕМЕТ		-ТБЗ-	ШУЛЕВ
	1	100				МОТОР		ПУНКТ			
	2	500		ДАНН.			ОТРЭД				
	3	1000			ИНСТРУКЦИ						
	4	1500									
	5	2000							ТУМАН	-АНТ-	ЮРЬЕВ
	6	2500	ВИДИМОСТЬ								
	7	3000		ДВИГАТЕЛЬ							
	8	3500									
	9	4000									

5

6

7

8

9

Appendix 12a.

Example showing use of the first general airforce code (1935—1937)
Original designation unknown.

(Russian 4-digit code).

Encipherment of the ten pages (columns in our version) by 1 to 10 different dinomes per page is irregular, changing on each network as deemed necessary.

The large digits 0—9 at the left margin are the tens, the 10x10 small digits 0—9 are the units for the rows.

Order of reading: Selectively one of the dinomes of the page involved (column) -- large figure at the left margin as 10 of the row -- small figure as unit of the row.

Russian plaintext:

КОМАНДИРУ 83. ЭСКАДР.
9 МАШИНЫ СЕЛИ БЛАГОПОЛУЧНО. ПРОШУ СООБЩИТЬ КОГДА ВЕРНУТЬ И ВЫСОТУ ПЕРЕЛЕТА.
НАЧАЛЬНИК АЭРОДРОМА ГОМЕЛЬ ПОНАМАРЕНКО

Translation: To the commander of the 83rd squadron.
9 machines landed smoothly.
Request instruction when and at what altitude return flight is to be made.
Commander of the Airfield Gomel.
Ponamarenko.

Cipher text with plaintext above:

КОМАНДИРУ	8	3	(•)	ЭСКАДР.	(•)	9	МАШИНЫ
3225	3780	8475	3758	7557	9058	5281	5177

СЕЛИ	БЛАГОПОЛУЧНО	(•)	ПРОШУ	СООБЩИТЬ	КОГДА	В	Е
6952	0439	8458	1485	4764	1321	5203	9013

Р	Н	У	Т	Ь	И	ВЫСОТУ	ПЕРЕЛЕТА	НАЧ.
3738	8424	5245	9042	8453	3717	7247	8925	6626

АЭРОДРОМА	ГО	М	Е	Л	Ь	ПО	НА	М
2923	3709	5223	9013	8421	3753	5234	9025	3723

А	Р	Е	Н	КО	(•)
9000	5238	8413	5224	8420	9058 —

13.(г)

4	7	0	ПЕРЕХОД, а/ом/у
5	8	9	ПЕРЕШ, ел/ла/ло/ли
6	9	8	ПЕРЕХОД, а/ом/у
7	0	7	ПОВТОРИТЕ
8	1	6	ПОГОД, а/е/ой/у
9	2	5	ПОКАЧИВАНИ, е/ем/и
0	3	4	ПОЛЕТ, а/ом/у
1	4	3	ПОРЫВИСТ.
2	5	2	ПОСАДК, а/и/ой/у
3	6	1	ПОСАДКУ ПРОИЗВЕ

67
05
25

0	5	6	РАДИОСВЯЗЬ
1	6	7	РАДИОСЕТЬ
2	7	8	РАДИОСТАНЦИ, ей/и
3	8	5	РАДИСТ, а/ом/у
4	9	4	РАЗВЕДК, а/ой/у
5	0	3	РАЗВЕДК. В НАПРАВЛ
6	1	2	РАЗВЕДК. ПРОТИВН.
7	2	1	РАЗВЕДК. ОБНАРУЖИЛ
8	3	0	РАЗВЕРНУ, лз/ак/ло
9	4	9	РАЗН.

73
98
29

8	2	9	ПОС. ПРОИЗВ. БЛАГОП
9	3	8	ПОС. ПРОИЗВ. НЕВОЗМ
0	4	7	ПОС. ПРОИЗВ. НЕМОГУ
1	5	6	ПОСЛЕ
2	6	5	ПОСТАВ, ила/ыла
3	7	4	ПРАВ.
4	8	3	ПРЕДСТАВ, ить/ыла
5	9	2	ПРИБУД, ет/ут
6	0	1	ПРИБЫЛ, а/и/о
7	1	0	ПРИЕМ

69
04
28

2	6	9	РАЗРЕША, ется/ются
3	7	8	РАЗРЕШИТЬ
4	8	7	РАЙОН, а/ом/у
5	9	6	РАЙОН ПЕРЕД. НАМК
6	0	5	РАЙОН ПРОТИВНИК
7	1	4	РАКЕТ, а/ой/у/ы
8	2	3	РЕЗУЛЬТАТ, а/ом/у
9	3	2	РЕЗУЛЬТАТ ДОНЕСТИ
0	4	1	РЕЗУЛЬТАТ. НЕТ.
1	5	0	РЕК, а/ой/у

74
97
30

13.(b)

70	6	1	7	ПРИКАЗ, а/ом/у
	7	2	6	ПРИЛЕТ, а/ом/у
02	8	3	5	ПРИЛЕТЕЛ, а/п/о
	9	4	4	ПРИНЯТЬ
	0	5	3	ПРИСТУП, ите/ить
	1	6	2	ПРОЛЕТ, а/ом/у
26	2	7	1	ПРОЛЕТЕЛ, а/п/о
	3	8	0	ПРОТИВНИК, а/ом/у
	4	9	9	ПРОШ, ел/ла/ли/ло
	5	0	8	ПРОШУ.

75	7	4	3	РЕМОНТ, а/ом/у
	8	5	2	РЕМОНТН.
96	9	6	1	РККА
	0	7	0	РОТ, а/ой/у/ы
	1	8	9	РОШ, а/п/у
32	2	9	8	РУССК.
	3	0	7	
	4	1	6	
	5	2	5	С
	6	3	4	САМОЛЕТ, а/ом/у/ы

71	3	0	1	ПУЛЕМЕТ, а/ом/у/ы
	4	1	0	ПУНКТ, а/ом/у/ы
	5	2	9	ПУТЬ
00	6	3	8	ПУШК, а/п/ой/у
	7	4	7	
	8	5	6	Р
28	9	6	5	РАБОТ, а/ы/ой/у/ы
	0	7	4	РАДИО
	1	8	3	РАДИОГРАММ
	2	9	2	РАДИОДАНН.

78	1	3	4	САМ.ПРОН.БЕЗЛЕТ
	2	4	3	САМОЛЕТ СЕЛ
94	3	5	2	САМСЕЛ БЛЯГОПОЛ
	4	6	1	САНИТАРН.
	5	7	0	СБИЛ, а/п/о
33	6	8	9	СБИТ, а/о/ы
	7	9	8	СБИТЬ
	8	0	7	СБОР, а/ом/у
	9	1	6	СВЕДЕНИ, а/ел/п/ей
	0	2	5	СВЕРХ

Appendix 13a.

Example showing use of the last general airforce system (section)

Original designation: "ВАК —38" = VAK - 38 Airforce code of 1938.

(Russian 3-digit code).

The VAK - 38 with some 800 groups is transmitted with 3 basic encipherments. These are designated black, red and green, in our diagram I, II, and III. The three dinomes standing in the outer box of our representation —

Left I = black,
Middle II = red
Bottom III = green — indicate, each color key separately, an ascending or decending sequence of dinomes. Since for 800 groups in 80 decades only 80 dinomes are required, 20 dinomes of each encipherment may be omitted at will. The single digit (in the decades) always remains unchanged in any color-key.

Encipherment is only by change of the dinome sequences and all three dinome sequences of the color keys are always changed simultaneously.

To illustrate the enciphering process we need only the section shown in the diagram (8 decades = 80 code groups = one-tenth of the entire code).

Russian plaintext:

САМОЛЕТ СБИТ ПРОТИВНИКОМ

Translation: Plane shot down by enemy

Cipher text within the three colored keys:

I (black):	756	786	703	-
II (red) :	963	948	028	-
III (green):	324	339	260	-

TOP SECRET

04	27
20	43
18	26
00	10
16	36
17	32
06	16
03	33
35	48
09	43
11	26
01	38
22	30
08	44
25	37
20	32
03	47
39	35
02	45
24	38
13	49
21	28
14	42
07	29
12	34

ДОВЕЛ, а/ли/о	ДОСТАВ, ить/ыть
ДОВЕСТИ	ДОСТАВЛЯ ет/ют
ДОГОВОР, а/ом/у	ДОСТАВЛЯТЬ
ДОЖД, ем/ь/ю	ДОСТИГ; ет/ют
ДОЗОР, а/ом/у	ДОСТИГ, ла/ло/ли
ДОКЛАД, а/ом/у	ДОСТИЖЕНИ, а/ем/и/ю
ДОКУМЕНТ, а/ом/у	ДОСТОЙН.
ДОЛ, гу	ДОСТУПН.
ДОЛОЖ, ите/ить	ДР
ДОМ, а/ом/у	ДРОВ, а/ь
ДОН	ДРУГ.
ДОНЕС, а/ом/у	ДУ
ДОНЕСИТЕ	ДЫ
ДОНЕСТИ	ДЫМКА
ДОНОШУ	
ДОНОШУ ЧТО	
ДОП	
ДОПОЛН.	Е
ДОПОЛНИТЕЛЬН.	ЕВ, а/ы
ДОПРАШИВ, ать/ять	ЕВ...
ДОПРОС а/ом/у	ЕГО
ДОР	ЕД, ет/ут
ДОРОГ, а/ой/у	ЕЕ
ДОРОГ. ХОРОШ.	ЕЖ, е
ДОРОГ. ПЛОХ.	ЕЖЕГОДН.../о

ЕЖЕДЕВИ.../о	ЕЦ
ЕЖЕМЕСЯЧН.../о	ЕЧ
ЕЖЕНЕДЕЛЬН.../о	ЕЩЕ
ЕЗ	ЕЮ
ЕЗД, а/ом/у	
ЕЙ	
ЕК	
ЕЛ	Ж
ЕМ	ЖЯ
ЕМКОСТЬ	ЖД
ЕМУ	ЖДАТЬ
ЕН	ЖДЕМ
ЕНМ, а/ему/и/ю/э	ЖДУ ВАШЕ УКАЗАН.
ЕНН.	ЖДУ ВАШЕ УКАЗАН.
ЕР	ЖДУ ОТВЕТ
ЕС	ЖЕ
ЕСЛИ	ЖЕЛЕЗ а/ом/у
ЕСЛИ БУД ет/ут	ЖЕЛЕЗН.
ЕСЛИ ЕСТЬ	ЖЕЛ.ДОРОГ, а/е/ой/у
ЕСЛИ НЕТ	ЖЕЛ.ДОРОЖН.
ЕСТЬ	ЖЕЛ.ДОР. МОСТ.
ЕСТЬ-ЛИ	ЖЕЛТ.
ЕТ	ЖЕН, а/ой/у
ЕТСЯ	ЖЕНЩИН, а/у/ы
ЕХАТЬ	ЖЕРТВ

			93	57	95	66	87		
		09	87	60	85	72	94	50	
	82	50	77	55	76	59	83	64	95	04
1	77	62	95	63	92	52	88	73	84	05
0	92	73	81	71	82	53	90	58	94	06
				А	61	90	67	78	53	91	07
				БЕЯ	67	87	55	95	60	82	08
				В	56	82	71	84	58	76	09
				ВО	60	97	57	98	70	67	10
				ВЫ	54	90	65	76	63	90	11
				Г	72	86	54	92	67	70	12
				ДЛЯ	59	78	61	85	59	86	13
				Е, Ж	50	91	68	96	62	83	14
					64	84	56	75	61	80	15
					58	98	73	86	65	78	16
					66	77	64	91	57	95	17
					53	89	62	80	72	98	18
					68	83	69	97	68	85	19
					61	94	50	77	74	97	20
					70	99	70	62	52	80	21
					52	75	63	89	11	92	22
					74	89	58	93	66	81	23
					62	88	50	79	69	99	24
					73	96	60	87	55	76	00
					65	79	74	99	58	96	01
					57	95	66	81	61	88	02
					69	85	72	94	50	77	03
					55	76	59	83	64	93	04
					63	92	52	88	73	84	05
					71	82	53	90	58	94	06
34	84	53	84		51	90	67	78	63	91	07
79	64	90			67	87	55	95	60	82	08
	71	75			56	81	71	84	54	75	09
		88			60	97	57	90	70		

TOP SECRET

Appendix 14a

Description of code and encipherment in connection with a page of the general commander code.

Original designation: "ОКК—5"
(Russian 4-digit code with substitution table.)

This code with some 5000 groups has 50 pages of 100 groups each in alphabetic-terminologic sequence. It consists of digraphs, letters, trigraphs, syllables, words, phrases, numbers from 00 to 99, marks of punctuation and cover groups for plane types as well as a few reserve cells. In the original the first 25 pages show an index at the right, the last 25 one at the left side of the page.

Encipherment is by two dinome substitution tables which are different for every net and can be interchanged arbitrarily. The substitution tables with some 12—18 dinomial substitution sequences each are numbered in sequence at the left and at the right margin and this numbering is always repeated twice either from 00 to 24 or 25 to 49 or from 50 to 74 or from 75 to 99. The two substitution tables differ from one another in that one table has sequences of the numbers from 00 to 49, the other has sequences from 50 to 99. Moreover the numbering of the double sequences (dinomes at the height of the line separating the sequences in the table) differs in the two tables.

The numbering of the lines and of the double sequences are the indicator components of the indicator group.

After setting up the correct pair of sequences as shown by the indicator group the substitution table is folded together and inserted in a pocket attached to the inside of the code book cover in such fashion that only the indicated double sequence remains visible. (Compare diagram -- left side of the code).

In order to demonstrate the use of the indicator group, the right side of the substitution table is shown as an unfolded fragment. It is clear that each sequence is introduced twice in succession, this is necessary in order to exhaust all possibilities of encipherment.

The position of the right hand substitution tables would correspond to the indicator group 3807--double sequences = 38, first line number = 07 — Of the left hand indicator group only the number 54 of the double sequence is visible since the sheet has been folded.

The two indicator groups are sent at the beginning of the cipher message, first the left and then the right.

Example: The page shown in the diagram has the alphabetic index "Е,Ж " which can be expressed enciphered by the number 50 or 91 (the index is on the same level with the dinomes). The word ДОНЕСИТЕ would read when enciphered: 5022 or 9122 (ДОНЕСИТЕ stands at the left in the outer column, hence the left hand substitution table, outer sequence), the word ЕСЛИ would be enciphered 5074 or 9174 (ЕСЛИ stands on the right in the other column, hence right hand table, inner sequence).

TOP SECRET

	42	75	03	64	29	10	86	31
07	АВИА	ВАШ, а/у	ДИРЕКТИВ, а/ой/у	ООО	НАСТУПЛЕНИ, а/ом/у	ПОМ.	СЕРЖАНТ, а, у	ЧЕРЕЗ
64	АВИАЦИ, ей/ю/ю/я	ВЗАИМОДЕЙСТВ.	ДЛЯ	КОМ. РОТ.	НАХОД, нтсв/нтся	ПОТЕРИ...	7	ЧТО
23	АВИАЦ, ПРОТИВ	ВЗВОД, а/ом/у	ДОЗОР, а/у	КОНТР.	3	ПОЧЕМУ	СНАЙПЕР, а/ом/у	ШТАБ, а/ом/у
91	АВТО	ТИРЕ(-)	ДОКЛАД, а/ом/у	КТО	НАЧ, альник	ПРЕДСТАВ, нть	СООБЩ.	ШТАДИВ
87	ЧИТ. ПЕРВ. БУК. СЛ.	ВИНТОВК, а/и	ДОНЕС, ите/ти	КУДА	НАЧАЛ, о	ПРИКАЗ, а/ом/у	СОСТАВ, а/ом/у	ШТАПОЛК
71	АВТОМАШИН.	ВОЕН.	О	ЛАГЕР	НЕМЕДЛЕНН	ПРОТИВНИК	СТАНЦИ, ой/и/ю	ШТАТ, а/ом/у
08	АГЕНТ, а/ом/у	ВОЕНН.	ДОРОГ, а/а/ой/у	ЧИТАЙТЕ СЛОВА	НЕМЕЦК	ПРОШУ	СТРЕЛКОВ.	ШТУК
52	АППАРАТ, а/ом/у	ВОСТОК	ДРУГ, ой	ЛЕВ.	НЕОБХОДИМ, о	ПТО	ТАНК, п	ЧИТАЙТЕ СЛОВА
39	ТЧК(.)	ВРЕМЯ	ЕЖЕДНЕВН. и/о	ЛЕЙТЕНАНТ, а/у	НОМЕР	ПУЛЕМЕТ, а/ом/у	ТЕРРИТОРИ, ой/и	ЭВАКУИР, овать
84	АРМИ, ой/и/ю/я	ВСЕ	ЗАДАЧ, а/а/у.	ЛЕС, а/ом/у	ОБЕСПЕЧ, нть/нт	5	ТОЛЬКО	ЭТ...
02	АРТИЯЯЕРИ	ВЫ	ЗАМ, ститель	1	ОБНАРУЖЕН, а/ы	ПУЛЕМЕТН	ТОЧН, о	ЮГ, о
25	АЭРОДРОМ, а/ом/у	ВЫСЛАТЬ	ЗАПАД	ЛИНИ, ой/и/ю/я	ОБЩ.	РАБОТ, а/ой/у	ТРЕБУ, ом/ю	
89	БАТАЛЬОН, а/ом/у	ВЫХОД	ЧИТ. ПЕРВ. БУК. СЛ.	ЛИЧН	ОЗЕРО	РАЗВЕДК, а/ой/у	ТРОФЕ, й/и	„ЗИС"
17	БАТАРЕ, й	ВЫЩ, ей/ю/ю/ю	ЗОНА	МАСЛ, о	4	РАЗРЕШ, ите	УБИТ, а/о/ы	„ГАЗ"
34	БЕЗИЗМЕН.	ГАРНИЗОН	ИМЕ, ем/ет/ю/ют	МАТЕРИАЛ, а/ом/у	ОРУДИ, е/ем/я	РАЗРУШ, нть	УДАР, а/ом/у	9
20	БЕНЗИН, а/ом/у	Д. ВТЧК(:)	ИНЖЕНЕР, н.	МАШИН, а/ой/у	ОТВЕТ, а/ом/у	РАЙОН, а/ом/у	УДАЧН.	„ФОРД"
41	БЕРЕГ, а/ом/у	ГДЕ	КАВАЛЛЕРИ, я	МЕСТ, о	ОТДЕЛ, а/ом/у	РЕЗУЛЬТАТ, а/у	8	
32	БОЕВ	ГОРОД, а/ом/у	КАПИТАН, а/у	МЕТР, ов	ЧИТ. ПЕРВ. БУК. СЛ.	РЕК, а/ой/у	УКАЗАНИ, е/ем/у	
78	ЗПТ(,)	ГОТОВ, ность	ОО	МЕХ.	ОТХОД, а/ом/у	РККА	УНИЧТОЖЕНИ, е/ем	„Т-34"
26	БО, ем/и/й/ю/я	ГОРЮЧ	КАРТ, а/ой/у	МИНОМЕТ, а/ом/у	ПАРТИ, йн.	РОТ, а/ой/у/ы	ФРОНТ, а/ом/у	„СТАЛИН"
11	БОЛЬШ.	ГРАНИЦ, а/ой/у	КИЛОМЕТР, ов	2	ПЕРИОД, а/ом/у	РУБЕЖ.	ФУГАЗН.	
45	БОЛЬШ. ПОТЕРИ	ЧИТАЙТЕ СЛОВА	КОГДА	МИНОМЕТН.	ПЕХОТ, а/ой/у	САМОЛЕТ	ХИМ, нческ	
59	БОМБ, нть/ет	ГРУПП, а/ой/у	КОМАНДИР	МОТОР, нст	ПЛЕН, н....	6	ХОРОШ, о	
19	БРИГАД, а/ой/у	ДЕЖУРН.	КОМ. БАТ.	МОТОРИЗОВАН	ПЛОХ, о	СВОДК, а/ой/у	ЧАС, ов	
63	БУД, ем/ет/ут	ДРОБЬ(/)	КОМ. ДИВ.	МЫ	ПОЗИЦ, И, ой/и/ю	СВЯЗ, н/ь	ЧАСТ, н/ь	
46	ВАМ	ДЕРЕВН, а/и/я	КОМ. БРИГ.	НАМ	ПОЛ, е	СЕВЕР	ЧИТ. ПЕРВ. БУК. СЛ.	
14	ВАС	ДИВИЗИ, ем/и/ю	КОМ. ПОЛК	НАС	ПОЛК, а/ом/у	ЧИТАЙТЕ СЛОВА	ЧЕЛОВЕК	

153

TOP SECRET

Appendix 15 a.

Example showing use of an SUV system (Regimental unit)

Original designation unknown (SUV)
(Russian 4-digit code)

This system has words, punctuation marks and the digits 0—9 and also contains 4x2 switch groups signifying

1. Read words

2. Read the first letter of the words.

Encipherment is by dinome substitution for elements AB and CD. Encipherment is at the discretion of the signal officer involved.

Russian plaintext:

НАЧ. ШТАБА 932. СТРЕЛКОВ. ПОЛК.

ПРОШУ СООБЩИТЬ ГДЕ КП ПОЛКА

ТИХОМИРОВ

Translation: To the Chief of Staff of the 932nd Infantry Regiment.
Please inform me of location of the regimental command post.
Tichomirov

Cipher text with plaintext above:
(Switch groups underscored).

ЧИТАЙТЕ СЛОВА НАЧ. ШТАБА Ч Э Ш (.) СТРЕЛКОВ. ПОЛКА

7545 2991 3123 3134 2923 6411 4239 8608 2914

(.) ПРОШУ СООБЩ. ГДЕ ЧИТ. ПЕР. БУК. СЛ. К П ЧИТАЙТЕ СЛОВА

4239 1008 8691 7541 0389 0359 1052 3152

ПОЛКА ЧИТ. ПЕР. БУК. СЛ. Т И Х О М И Р О В

2914 2932 8602 0320 8645 2934 6478 0334 1041 2934 7525

TOP SECRET

	01	02	03	48	49	50
01	5	(,)	БИЛЕТ, а/мо/у	Ф	ЧЕРЕЗ	Щ,
02	А	(.)	БИНОКЕЛ, ь	ФА	ЧЕТВ	Щ,А
03	АБ	АНГЛИСК.	БИО	ФАБРИКА	ЧИ	Щ,Е
04	АБЗАЦ	АНИ, е/ем/и/ю/я,	12	ФАКТ, а/ом/у	ЧИСЛ, о	Щ,И
05	АВ	АП	БИОГРАФИ, ей/п/ю/я,	ФАКТИЧЕСК.	ЧО	(.)
06	АВАНГАРД, а/ом	АППАРАТ, а/ом/у	БЛ	ФАМИЛИ, ей/п	ЧТО	(,)
07	АВАРИ, ей/и/ю/я,	АПРЕЛ, ь/я,	БЛАГ, о	ФАШИСТ	ЧУ	Ы
08	АВГУСТ	АР	БЛАГОПОЛУЧН.	ФАШИСТСК	ЧУЖ, ой	ЫВ
09	АВИА	АРЕСТ	БЛАНКО	ФЕ		ЫВАЕТ, ся
10	АВИАЦИ, ей/и/ю/я	АРЕСТОВАН, а/о/ы	14	ФЕВРАЛ, ь/я,		ЫВАЙТЕ
11	АВТО	10	БЛИЖАЙШ.	ФЕЛЬДВЕБЕЛЬ	(,)	ЫЕ
12	АВТОБЕНЗИН	АРМИ, ей/и/ю/я	БЛИЗК.	ФЕЛЬДШЕР	(.)	ЫЕМ
13	АВТОМАШИН	АРТИЛЕРИ ей/и	БЛИНДАЖ	ФИ		ЫЕТ
				Ф ИЧЕСК		Ы
			АРБА			
36	О	БЕ	БАНДАРЕНКО		ШОФФЕР, ау	Я,В...
37	АЗ	БЕЗ	БОЛТАЕВ		ШТАБ а/ом/у	Я,ВNТСЯ,
38	АЙ	БЕЗ ДОКУМЕНТ.	БОРОДИН	Ч	ШТАТ, а/ом/у	Я,Д
39	АЙТЕ	БЕЗ ВЕСТИ	БУРЛАКОВ	ЧА	ШТУК, а/и	Я,ЕМ
40	АК	8	БЫСТРЫЙ	ЧАС, а/ов	ШТУРМ, ов	Я,ЕТ
41	АККУМУЛЯТОР	БЕЗ ИЗМЕН	(,)	ЧАСТ, и/ь/ью	ШУ	Я,ЕТСЯ,
42	АКТ, а/ом/у	БЕЛ, о	(.)	ЧАСТ, я м/я х		Я,И,Те
43	АКТИВ	БЕНЗИН, а/ом/у	17	ЧЕ	ЧЕРЕБАНОВ	Я,К
44	2	БЕР	БОТИН, кн	ЧЕВ	ШУВАЛОВ	Я,М
45	АКТИВН	БЕР, ет/ут	БОУ ск/ка/кн	ЧЕЙ	ШУРИН	Я,НВАР ь/я,
46	АКТИВНОСТЬ	БЕРЕГ, а/ом/у	БР	ЧЕЛОВЕК, а/ом	Я,БЛИК	Я,СН, о
47	АЛ, и	БЕС	БРИ	ЧЕМ	Я,СНОВСКИЙ	Я,ЩИК, а/ом/п/у
48	АМ	11	БРИГАД, а/ой/у	ЧЕМУ		Я,Ю
49	АМЕРИКАНСК	БЕСПАРТИЙН	БРО	ЧЕНИ, е/ем/и/ю/я,		Я,ЮТ, ся
50	АН	БИ	БРОНЕМАШИН	ЧЕР, н		Я,Я,

TOP SECRET

Appendix 16a.

Description of codes and of encipherment showing use of a (fragmentary) code table of NKVD border and security troops.

Original designation "ЗЕРНО" = SERNO
(Russian 4-digit code enciphered with substitution sequences)

The partial reproduction of this 4-place alphabetic—terminologic code table with 250 groups (50 pages of 50 groups each), shows the numbering of pages and lines of the basic code.

The code contains letters, digraphs, trigraphs, syllables, words, numbers from 0 to 31 (corresponding to day dates, marks of punctuation (with variants) and cover groups for surnames of military and political leaders (differing in each net).

The pages 01 to 50 and the lines 01 to 50 of the basic code are enciphered by two different dinomial substitution sequences. Each page and line of the basic code can therefore be expressed in two different ways since 2x100 different dinomes (00 to 99) are available for only 50 pages and 50 lines of the basic code.

Example:

Let us assume that page 49 can be replaced by either 17 or 42 and line 37 by either 94 or 38, then for example the word ШТАБ can be replaced in 4 different ways, namely 4794, 4738, 1794 or 1738.

Appendix 17

Example of additive encipherment (operational-tactical code, general table).

ОБЩИЙ БЛОКНОТ НР. 07043

14	37	49	51	60	78	81	86	93	95	
437	95024	67014	35801	86731	00845	38609	46836	78211	96474	48708
452	01184	75903	27804	73861	37011	57379	46830	28455	86649	43208
489	75904	66279	86451	17410	85047	65793	60141	58309	47562	38594
507	19405	83922	47605	76839	46017	83447	99270	05001	37096	32581
541	06397	82491	15408	.....	.....	.....	.....	.....	.....	.....
753	.....	.....	etc. a total of 30 lines of ten 5-digit groups.							

Plaintext with intermediate text (encoded text), indicator group (starting point) line 437, column 78 = 43778

ПРОДОЛЖЕНИЕ ПЕРВОЕ ШИФРТЕЛЕГРАММЫ НР. 17 04 (-) 2. 917.

76240	96485	00914	00287	09713	90916
СТРЕЛКОВЫЙ ПОЛК ОБОРОНЯЕТ ПРЕЖНИЙ РУБЕЖ (-) [КОМ. ДИВИЗИЙ					
87325	54130	73980	82321	43299	42636
272. С.Д. И 190. С.Д. (—) НАЧ. ШТАБА АРМИИ] 3.					
69348	37284	49737	12869	50952	59892
АВИАЦИЯ ПРОТИВНИКА					
00473	.....	..... etc.			

Translation: First continuation of enciphered message No. 1704.
2. The 917 Infantry Regiment defends the former (old) Sector.
[To the Division Commanders of the 272nd and 190th Infantry Division--Chief of Staff of the Army]
3. The enemy airforce .....

Encipherment of the intermediate text with the additive sequence of the above Bloknot (indicator in third position, Bloknot number in second position):

76240	07043	43778	96485	00914	00287	09713	90916	87325	54130	73980	82321	43299
38609			46836	78211	96474	48708	01184	75903	27804	73861	37011	57379
04849	07043	43778	32211	78125	96651	47411	91090	52228	71934	46741	19332	90568

42636	69348	37284	49737	12869	50952	59892	00473
46830	28455	86649	43208	75904	66279	86451	17410
88466	87793	13823	82935	37763	16121	35243	17883 = Cipher text

Note: Address and signature are generally placed in the middle of the message between square brackets.

Appendix 18a

Partisan, scout and agent systems.
One and two place substitution with a key word
(Russian one and two place substitution).

The encipherer and decipherer need no key document. It is only necessary to remember the key word, in this case САМОЛЕТ = airplane and to construct the matrix from this whenever necessary. The letters of the key word are numbered alphabetically beginning with 1.

Key word: С А М О Л Е Т

Numerical key: 6 1 4 5 3 2 7

These seven letters of the key word are then the one digit elements of the substitution. The unused digits 8, 9, and 0 are used as the tens of the cipher digraphs for the missing letters and marks of punctuation.

Substitution:
(Cäsar:)

А = 1	Ж = 84	Н = 88	У = 91	Щ = 97	(.) = 03
Б = 80	З = 85	О = 5	Ф = 92	Ъ = 98	(,) = 04
В = 81	И,Й = 86	П = 89	Х = 93	Ы = 99	
Г = 82	К = 87	Р = 90	Ц = 94	Э = 00	
Д = 83	Л = 3	С = 6	Ч = 95	Ю = 01	
Е = 2	М = 4	Т = 7	Ш = 96	Я = 02	

Sample encipherment

Russian plaintext: Я РАНЕН КОНЧАЮ РАБОТУ

Translation: I am wounded (I) am ending the work.

Cipher text:

02901882888758895101901805717980З -

Note: The cipher text can be divided up in any desired fashion and may be transmitted backward.

Appendix 18 b

Partisan, scout and agent systems.
Sample of a double transposition with example.

The double transposition is a combined double transposition system. Decipherment is possible only with the aid of complete or partial compromises.

Enciphering and deciphering is handled the same as with single transposition, the cipher text obtained from the first box is treated as intermediate text and enciphered again by the second box. The two boxes must have different widths.

Example:

The plaintext is inscribed in the first box from left to right, line by line, and the cipher text (intermediate text) is taken out by columns following the numerical key. This intermediate text is inscribed in the second box and the final cipher text is taken out in the manner described above.

Russian plaintext:

ШТАБ СТОПЯТОЙ НЕМЕЦКОЙ ДИВИЗИИ НАХОДИТСЯ В ДЕРЕВНЕ ЙЕНАЯ ДРУГИХ ПЕРЕМЕН НЕТ ШУРА

Translation: The Staff of the 105th German division is in the village Jasnaja. Otherwise no changes. Schura.

1st phase of encipherment (box 1):

Key word: Г О Р О Д В И Т Е Б С К

Numerical key: 3 8 10 9 4 2 6 12 5 1 11 7

Ш	Т	А	Б	С	Т	О	П	Я	Т	О	Й
Н	Е	М	Е	Ц	К	О	Й	Д	И	В	И
З	И	И	Н	А	Х	О	Д	И	Т	С	Я
В	Д	Е	Р	Е	В	Н	Е	Я	С	Н	А
Й	Д	Р	Ъ	Г	И	Х	П	Е	Р	Е	М
Е	Н	Н	Е	Т	Ш	У	Р	А			

Appendix 18 b
(continued)

Intermediate text:

ТИТСР ТКХВИ ШШНЗВ ЯЕСЦА ЕГТЯА ИЯЕАО ООНХУ

ЙИЯАМ ТЕNДД НБЕНР УЕАМИ ЕРНОВ СНЕПЙ ДЕПР-

2nd phase of encipherment (box 2)

Key word: С М О Л Е Н С К

Numerical key: 7 4 6 3 1 5 8 2

Т	И	Т	С	Р	Т	К	Х
В	И	Ш	Ш	Н	З	В	Я
Е	С	Ц	А	Е	Г	Т	Я
Д	И	Я	Е	А	:	С	О
Н	Х	У	Й	И	Я	А	М
Т	Е	И	Д	Д	Н	Б	Е
Н	Р	У	Е	А	М	И	Е
Р	Н	О	В	С	Н	Е	П
Й	Д	Е	П	Р			

Cipher text: РНЕАИ ДАСРХ ЯЯОМЕ ЕПСША ЕЙДЕВ

ПИИСИ ХЕРНД ТЗГОЯ НМНТШ ЦЯУИУ

ОЕТВЕ ДНТНР ЙКВТО АБИЕ-

Appendix 18c

Partisan, scout and agent systems.

Example showing use of the grille [Raster].

Grilles are transposition systems. Two types of grilles are distinguished:

1. the revolving grille

2. the ordinary grille (with blind cells)

The revolving grille is little used and will not be described in detail here since it has never been recognized in Russian traffic.

The ordinary or simple grille belongs among the complicated transposition systems and when the rules for encipherment are followed precisely can only be solved by the aid of complete or partial compromises.

Example of the small grille.

The 100 letter grille below has 18 columns and 10 lines, each line has 8 blind cells which are differently located in each line. The numerical key is derived from a key word of 18 letters (= the number of columns). The plaintext is inscribed from left to right, line by line, in the open cells (10 in each line). The cipher text is then taken out by columns starting with column 1 (see numerical key).

Russian plaintext:
ШУРА УБИТ ИЛИ ВЗЯТ В ПЛЕН. ЧТО ДЕЛАТЬ? БУДУ РАБОТАТЬ ЗАПАСНОЙ ШИФРОЙ. ДАЙТЕ УКАЗАНИЕ. МИША

Translation: Schura has been killed or captured.
What shall I do?
I shall work with the reserve cipher
Give instructions.
Hischa.

Appendix 18 c
(continued.)

Message in the grille:

Key word:

	О	Т	Е	Ч	Е	С	Т	В	Е	Н	Н	А	Я	В	О	Й	Н	А
Key:	12	15	5	17	6	14	16	3	7	8	10	1	18	4	13	8	11	2

	Ш	У		Р		А	У	Б		И		Т			И		Л	
И		В	З			Я			Т		В	П	Л	Е			Н	
	Ч		Т	О	Д		Е	Л		А		Т			Ь	Б		
	У	Д		У		Р		А		Б	О		Т	А			Т	
Ь			З		А	П	А		С		Н		О		Й	Ш		
И		Ф	Р	О	Й			Д		А				Й		Т	Е	
У	К			А			З		А		Н	И	Е		М		И	
Ш		А																

Cipher text:

ВОННЛ НТЕИУ ЕАЗЛТ ОЕУВА ФАРОУ ОАБЛА

ДИЬЙМ ТСАИА БАБШТ ИЬИУШ ЕАЙДА ЙШЧУК

АЯРПЗ ТЗРТП ТИ-

Appendix 18 d.

Partisan, scout and agents system

Additive encipherments.

Aside from additive encipherments such as were used in the army, airforce, and NKVD, partisan, scout, and agent traffic employed primarily so-called additive rolls. These were rolls of paper tape of considerable length (several meters) bearing a sequence of random digits. The portion of tape used to encipher or decipher a message was torn off and destroyed thus insuring that one and the same number-text was used only once for encipherment since each roll was prepared in only two copies, one for the receiver and one for the sender.

There is no need to debate the absolute security of this "individual" use, decipherment is absolutely impossible even though the system itself is known by capture. It does not matter whether the message thus enciphered was originally put through a code or a simple substitution.

Most frequently substitutions of the type described in appendix 18a were reenciphered by additive rolls.

Example of encipherment:

Intermediate text (cipher text of 18a) with additive written out beneath:

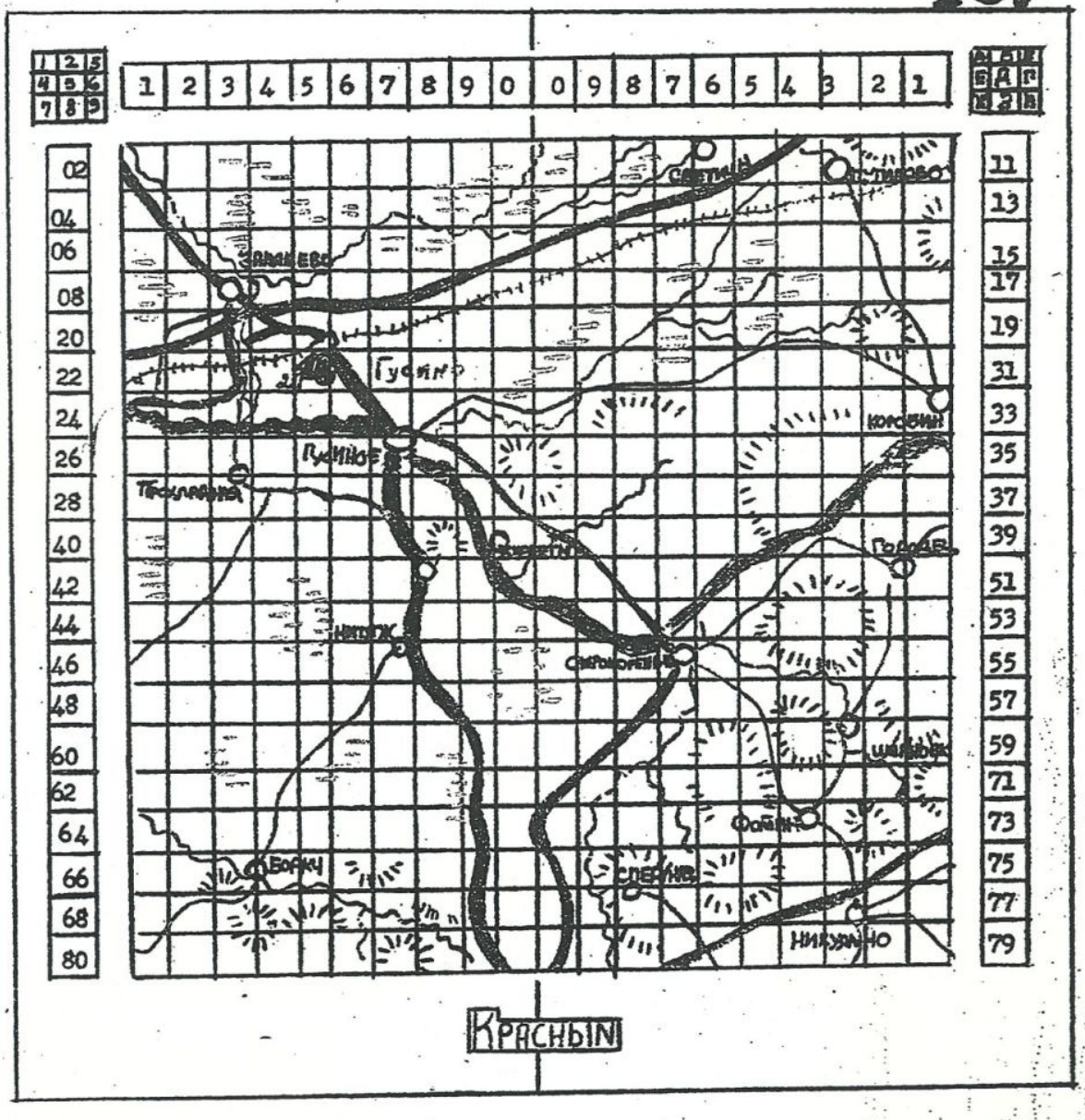
02901882888758895101901805717980 3 -

840624815710603317407924004869414085990356 1

Cipher text: 869632633597181268416932051938217

Note: Division into groups optional

19.


1 2 3 4 5 6 7 8 9 0 0 9 8 7 6 5 4 3 2 1
02 04 06 08 20 22 24 26 28 40 42 44 46 48 60 62 64 66 68 80
11 13 15 17 19 31 33 35 37 39 51 53 55 57 59 71 73 75 77 79
Гусино
Гусиное
Коробин
Борку
Никулино
Красный

Appendix 19a.

The map planchette and its use.

The reproduction of a Russian map planchette, scale 1:1.5, with a map section of the area southwest of Smolensk will serve to illustrate the method of encipherment.

The area of the map 1: 100,000 visible under the grid represents 20x20 km, each of these 400 square kilometers may be expressed by a three digit number -- a dinome from the left or right margin, a monome from the upper margin of the planchette. The area of 1 square kilometer can be subdivided when necessary according to the key given in the upper left or upper right corner.

On maps suitable for this planchette the names of cities of over 10,000 inhabitants are underscored and also indicated by a 2-digit number. This number is the key for applying the planchette. The area in question, i. e. the actual map sheet, is assumed to be known.

If one coordinate reads for instance 39512, the decipherer knows that he must look up on the appropriate map sheet the city designated by the number 39 (the first two digits of the coordinate). When he has found this he lays the planchette on the map so that the city name is visible in the window at the bottom of the planchette, the initial letter (in larger print) must cut off precisely at the left margin of the window. Now the coordinate can be read, the planchette itself is oriented to the North.

Assuming that the city name КРАСНЫЙ has the ordinal 39, the town ГОРОДЕЦ lies in the area 39512. Or: the bridge over the Dnieper at the south exit of the town ГУСИНОЕ has the coordinate 39267, or more precisely 392672 or 29267 Б .

Appendix 20

Explanation of technical terms.

alphabetisch	(alphabetic) applies to a [one part] code which is in absolute alphabetic and terminologic sequence like a dictionary.
aufgebrochen-alphabetisch	(interrupted alphabetic) applies to a code where entries with like initial letter are in alphabetic sequence but the sequence of the initial letters does not correspond to the normal alphabet.
Belegung	Is the position (cell) in a code assigned to a letter, a bigram or some other concept.
Bigramm	Is a pairing of letters or digits.
Blender	(null) is a blind element in enciphered text, sometimes a bigram, trigram, or even an entire group, which is inserted in the cipher text either to render unauthorized decipherment more difficult or merely to fill out a unit.
Cäsar	Is the simplest type of substitution system still used at the present time. The plain elements of a message, the letters, digits and marks of punctuation, possibly also the most frequent bigrams, are replaced by various combinations of letters or numbers or both, usually in the form of bigrams.
Chi	Is the abbreviation for Chiffre, chiffrieren or chiffriert.
Chielement	(cipher element) is the smallest unit, a single digit or a single letter, of a cipher group.
Chiffrant	Is a copy of a code for enciphering, that is with alphabetic but not terminologic sequence of the code positions.
Chigruppe	(Cipher group) is a group of the enciphered text.
Chispruch	Is an enciphered message.
Chitext	Is an enciphered text.
Code	Is a substitution system of relatively large extent containing, aside from letters, digits and marks of punctuation (often with variants), bigrams, trigrams, syllables, words and compound concepts, type designations and cover groups.
Dechiffrant	Is a copy of a code for deciphering, i. e. with the code positions in terminologic but not in alphabetic sequence.

Deckgruppen (cover groups) are positions of a code which may signify among other things given names and family names, city names, official positions, troop units, unit numbers, etc.

Element of a cipher group -- see Chielement.

Entschlüsseln (decipherment) is the removal of the camouflage from enciphered material by the use of regular keys etc. in contrast to Entziffern (decrypting).

Entzifferung Is the activity which may lead to the unauthorized reading of enciphered material. It removes the camouflage from the cipher material without being in possession of keys etc. by recovering these. The concept "Ziffer" is used in this word only in an abstract sense.

Ersatzverfahren (Substitution systems) are cryptographic systems in which the plain element or the plain concept is replaced by combinations of digits, letters or both, which by themselves would have a different value.

Erweiterte Cäsaren (Expanded substitutions) contain, aside from letters, digits and marks of punctuation, bigrams, syllables, short words and sometimes 2-digit numbers. In contrast to the simple Cäsar the number of cells may exceed 100.

Ez. Abbreviation for Entzifferung. (decipherment -- cryptanalysis)

Feld = Position or Belegung.

Häufigkeit (frequency) is in general the percentual frequency of occurrence of letters, bigrams, etc., in a language.

Hinweisgruppe (switch group) is a group indicating the manner of reading.

Indikator (indicator) usually means the same as Kenngruppe, but aufgeschlüsselt or gegliedert [?]
Indikator may also mean only a part of the Kenngruppe.

Kenngruppen (indicator groups) are groups which almost without exception are found among the first ten or last ten groups of a cipher message and which indicate the encipherment including the starting point if necessary.

Kenngruppen may be sent in clear or camouflaged, i. e. enciphered.

Kettenstatistik
(index) is a count which shows not merely the frequency but also the cipher group following the indexed group in the text.

kombinierte verfahren
(combined systems) are systems combining two or more encipherments, e. g. substitution-substitution, transposition-transposition, substitution-transposition or transposition-substitution.

Kontrollgruppe (control group) is a second Kennegruppe Either like to or supplementing the first.

mehrfach belegt
Applies to a code which allots two or more code groups for frequent plaintext meaning. [with variants]

Monogramm Is a single letter or a single digit.

Position = Feld or Belegung, the smallest unit in the structure of a code (Ersatzverfahren).

Satzbuch (code) is an especially large code with entire sentences (commercial, economic and diplomatic codes).

Schlüsselmittel
are cryptographic systems, methods of camouflage, systems of reencipherment and documents pertaining thereto.

schlüsseln or verschlüsseln
(encipher) is the disguising of plaintext by the aid of means of encipherment, i. e. the transformation of plaintext into cipher text.

Spaltencäsar (polyalphabetic substitution) is a cryptographic system using several Cäsaren. The individual alphabets are used one after the other in rotation. Encipherment with numerous cipher machines is based on this principle of the so called expanded Tritheim method (Tritheim was a Benedictine Abbot in the 16th century)

symbolische Addition
Is the addition of two digits without carrying the tens [mod 10].

Tauschverfahren
(substitution systems) are a limited category of substitution systems beyond the frame work of the two place Cäsaren. All systems with bigram substitution, mixed substitution and monogram substitution with at least three elements are termed Tauschverfahren.

Appendix 20
(continued)

terminologisch
(terminologic) signifies a directly or indirectly ascending or decending sequence of numbers.

Trigramme — are combinations of letters or digits having three elements.

Umfang — signifies the total number of positions (Felder or Belegungen) of a code.

Versatzverfahren
(transpositions) are cryptographic systems where the plain elements are scrambled by certain regular changes of position (i.e. are transposed).

Würfel — is the simplest transposition system still used at the present time where the plain elements are inscribed in a rectangle from left to right, line by line, and are then taken out, column by column, according to a key and divided into groups of any desired length.

Turm or Zählenwurm
(additive sequence) is an unsystematic, practically endless numerical sequence which is added mod 10 as reencipherment to a numerical enciphered text.

Appendix 21

Compilation of systems of the army, airforce and NKVD 1935--1941 which were in use for somstime and were decrypted.

(Down to the outbreak of the Russo-German war.)

1. Original designation: "PT -- 35" (chatter table of 1935)

General designation: First general operational system of army and airforce.

Message groups: 2-digit (sometimes sent in 4-digit groups)

Formula: R2ZCr. (Russian 2-digit Cäsar)

Structure: 2-digit Cäsar with 100 positions. Letters in alphabetic sequence, 1-digit numbers, marks of punctuation and selected operational-technical and tactical terms.

Encipherment: System squares for single digit substitution for the tens and units.

Area of use: Army and airforce generally, from division down.

Message content: Primarily operational, internal service and personnel matters. During maneuvers also tactical content.

Period of use: October 1936 to September 1939.

Predecessor: Various small Cäsaren of short duration, for army and airforce.

Successor: "PT--39" (see 2.)

Traffic receipts: Heavy receipts primarily in the Western military districts, materially heavier during maneuvers.

Readability: Homogeneous material of at least 50 groups read in full.

Remarks: None

2. Original designation: "PT -- 39" (chatter table of 1939)

General designation: Second general operational system of army and airforce.

Message groups: 2-digit (sometimes sent in 4-digit groups)

	Formula:	R2ZCr. m. tlw. dop. Lsart. (Russian 2-digit Cäsar with some cells having two meanings).
	Structure:	2-digit Cäsar with 145 positions. Some cells have two meanings, shown by two switch groups ("read letters" "read words") Otherwise like 1.
	Encipherment:	Like 1
	Area of use:	Like 1
	Message content:	Like 1.
	Period of use:	October 1939 to February 1942.
	Predecessor:	"PT—35" (see 1)
	Successor:	"PT-41" (see appendix 22—1).
	Traffic receipts:	As for 1
	Readability:	As for 1
	Remarks:	None
3.	Original designation:	Unknown
	General designation:	General and operational system of the border guard district (NKVD) Leningrad, Nord, and Kasakstan.
	Message groups:	Bigrams consisting of 1 digit and 1 letter.
	Formula:	RZBCr. (Russian digit-letter-Cäsar)
	Structure:	2-place digit-letter-Cäsar with alphabet, digits, and marks of punctuation. Values of the remaining cells (theoretically 100 positions different in each of the three nets.
	Encipherment:	Monogram substitution using two system squares (a digit square for the tens, a letter square for the units).
	Area of use:	NKVD border guard troops of the border guard districts Leningrad, Nord and Kasakstan.

	Message content:	General affairs of border guard troops.
	Period of use:	End of 1934 to February 1939.
	Predecessor:	Probably none, since this was the first NKVD cryptographic system for the border guard troops.
	Successor:	For messages of operational content the first general NKVD operational system (see 7); for messages of organizational and tactical content the first general NKVD code for border guard and security troops (see 18).
	Traffic receipts:	Various. Depending on the season. In summer Kasakstan could be heard well, in winter Nord and Leningrad. Rarely more than 10 messages a day.
	Readability:	As for 1.
	Remarks:	None.
4.	Original designation:	Unknown
	General designation:	General and operational system of the coast guard Odessa.
	Message groups:	5-digit groups; two 2-digit groups, middle digit a null. Cipher group: 2-digit.
	Formula:	R2ZCr. m. Bl. (Russian 2-digit Cäsar with nulls).
	Structure:	2-digit Cäsar with 100 Positions, some being reserve cells. Alphabet, digits, marks of punctuation, and selected words as under 1.
	Encipherment:	Like 1.
	Area of use:	NKVD border guard troops of coast guard district Odessa.
	Message content:	Like 3.
	Period of use:	October 1935 to February 1939.
	Predecessor:	Probably none.

	Successor:	As under 3.
	Traffic receipts:	Average: 5-messages daily.
	Readability:	As for 1.
	Remarks:	None
5.	Original designation	Unknown
	General designation:	General and operational system of coast guard Novorossisk.
	Message groups:	6-digit, three 2-digit cipher groups.
	Formula:	R2ZCr. (Russian 2-digit Cäsar)
	Structure:	2-digit Cäsar with 100 Positions, some being reserve cells. Alphabet, digits, punctuation marks, and selected words as under 1.
	Encipherment	Like 1
	Area of use:	NKVD border guard troops of coast guard Novorossisk.
	Message content:	Like 3.
	Period of use:	October 1935 to February 1939.
	Predecessor:	Probably none.
	Successor:	As under 3.
	Traffic receipts:	Light, 20 messages a month at most.
	Readability:	As under 1.
	Remarks:	None
6.	Original designation	Unknown
	General designation:	General and operational system of the border guard district Transcaucasus.
	Message groups:	5-digit (containing either 5 tens or 5 units of the 2-digit cipher groups)
	Formula:	R2ZCr. erw. m. Verst. (Russian 2-digit Cäsar expanded with trans-position).

	Structure:	Expanded 2-digit Cäsar with 100 positions. Alphabet, bigrams, syllables, frequent short words, digits, marks of punctuation, and selected words as under 1.
	Encipherment:	Like 1 Also transposition by separation of the tens and units. (see appendices 10 and 10a)
	Area of use:	NKVD border guard troops of the district Transcaucasus.
	Message content:	Like 3.
	Period of use:	January 1936 to February 1939.
	Predecessor:	Probably none
	Successor:	As for 3.
	Traffic receipts:	Heavy, depending on the season. Average: 10 messages a day.
	Readability:	As for 1.
	Remarks:	None
7.	Original designation:	Unknown
	General designation:	First general operational system of the border guard troops NKVD.
	Message groups:	Like 1.
	Formula:	R2ZCr. (Russian 2-digit Cäsar)
	Structure:	Like 1
	Encipherment:	Like 1
	Area of use:	NKVD border guard troops generally.
	Message content:	Operational -- technical reports.
	Period of use:	March 1939 to May 1945.
	Predecessor:	Cäsaren of the border and coast guard districts Leningrad, Nord, Kasakstan, Odessa, Novorossijsk and Transcaucasus.

	Successor:	Not known
	Traffic receipts:	Heavy in the years before the war, later light, in the last two years only isolated messages.
	Readability:	As for 1.
	Remarks:	None
8.	Original designation:	Unknown
	General designation:	First operational system for internal Russian traffic.
	Message groups:	Like 1
	Formula:	R2ZGr. (Russian 2-digit Cäsar)
	Structure:	2-digit Cäsar with 45 positions. Alphabet, digits, and marks of punctuation, no words.
	Encipherment:	Like 1.
	Area of use:	Nearly all major radio stations for internal traffic.
	Message content:	Matters dealing with operations and communications technique.
	Period of use.	1935—1938
	Predecessor	Unknown
	Successor:	Unknown.
	Traffic receipts	Not part of our assignment, stray messages were picked up.
	Readability:	Like 1
	Remarks:	None

9.	Original designation:	Unknown
	General designation:	First code of the NKVD border guard troops Kasakstan.
	Message groups:	4-digit
	Formula:	R4ZC (Russian 4-digit code).
	Structure:	4-digit code with 25 pages of 100 positions each (2500 positions in all). Contained alphabet, bigrams, trigrams, syllables, words, numbers from 00 to 99 and punctuation marks.
	Encipherment:	Dimone substitution for pages of the basic code.
	Area of use:	NKVD border guard troops Kasakstan.
	Predecessor:	Cäsar of border guard Kasakstan (see 3).
	Successor:	Second code of NKVD border guard troops Kasakstan (see 17).
	Message content:	General matters of the border guard and press-reports.
	Period of use:	December 1935 to March 1937
	Traffic receipts:	Various, heavy in the summer months.
	Readability:	Homogeneous material of at least 100 groups read in full since the middle of 1936.
	Remarks:	None
10.	Original designation:	Unknown
	General designation:	First general air code
	Message groups:	4-digit
	Formula:	R4ZC. (Russian 4-digit code)
	Structure:	4-digit code with 10 pages of 100 Positions each (1000 Positions in all). Auxillary alphabet with bigrams and most frequent syllables, digits and selected numbers for flying elevation. Words of air technical character and for weather reports. Cover groups for types of planes and proper names. Reserve cells.

Encipherment:	Dinome substitution for pages of the basic code. Each page can be expressed in as many as 10 different ways for any encipherment.
Area of use:	Airforce in general
Predecessor:	Various small Cäsaren and codes of short life over limited areas.
Successor:	"VAK-38" (see 14).
Message content:	Take off and landing reports, weather reports, internal service, personnel matters, organization and development as well as tactical messages during maneuvers.
Traffice receipts:	Varied, sometimes heavy, up to 50 messages a day.
Period of use:	1935 to November 1938. After recovery late in 1935, homogeneous material of at least 30 groups could be read in full.
Remarks:	None

11. Original designation: Unknown

General designation:	First airforce parade and maneuver code of 1 May 1936
Message groups:	3-digit
Formula:	R3ZC. (Russian 3-digit code)
Structure:	3-digit code with 6 pages of 100 Positions each (600 positions in all), otherwise like 10.
Encipherment:	Monogram substitution for all elements (hundreds, tens, and units).
Area of use:	All airforce formations, ground organizations, air fields etc. which stand in direct or indirect connection with the May parade in Moscow.
Message content:	All matters connected with the air parade.
Period of use:	Air parade Moscow (May 1936) mid April to mid May 1936.

Predecessor:	None
Successor:	Second air parade and maneuver code of 1 May 1937.
Traffic receipts:	Especially in the days around 1 May very heavy, up to 200 messages a day.
Readability:	After recovery, homogeneous material of at least 30 groups could be read in full in a few days.
Remarks:	None

12 and 13. Like 11. Little changed, somewhat expanded from year to year.

12. Second airparade and maneuver code 1937
13. Third airparade and maneuver code 1938.

14. Original designation:	"VAK-38" (airforce code of 1938)
General designation:	Second General airforce code.
Message groups:	3-digit
Formula:	R3ZC (Russian 3-digit code)
Structure:	3-digit code with 80 decades of 10 positions each (800 positions in all) Auxillary alphabet, air technical and meteorological terms and compound concepts, numbers 0—9 and flight elevations, punctuation marks and cover groups.
Encipherment:	3 basic encipherments black, red and green. Dinome encipherment of the hundreds and tens. Units constant within the basic encipherment.
Area of use:	Airforce in general.
Message content:	Various, principally operations and communications, take off and landing reports and weather service.
Period of use:	November 1938 to December 1939.

	Predecessor:	First general airforce code (see 10)
	Successor:	Various small codes and chatter tables of short life, in very limited areas. For tactical matters the first large code for army and airforce (19)
	Traffic receipts:	Varied, generally light.
	Readability:	After recovery of the system early in 1939 homogeneous material of at least 30 groups was completely readable.
	Remarks:	None
15.	Original designation:	Unknown
	General designation:	First army code of the military district Moscow
	Message groups:	4-digit
	Formula:	R4ZC (Russian 4-digit code)
	Structure:	4-digit code of 20 pages with 100 Positions each (2000 positions in all). Alphabetic-terminologic sequence. Alphabet, bigrams, trigrams, syllables, words, numbers from 00 to 99, punctuation and some cover groups for proper names.
	Encipherment:	Dinome substitution for the thousands and hundreds (AB), monogram substitution for tens (C), units (D) unchanged.
	Area of use:	Army, military district of Moscow, corps to regiment.
	Predecessor:	None
	Successor:	First relatively large code for army and airforce (see 19).
	Period of use:	July 1936 to May 1937
	Message content:	Tactical content, internal service, personnel affairs, organization etc.
	Traffic receipts:	Varied. Very heavy during two maneuvers, otherwise only scattering.

	Readability:	After recovery of the system homogeneous material of at least 100 groups completely readable.
	Remarks:	None
16.	Original designation:	Unknown
	General designation:	First general NKVD code (reserve system)
	Message groups:	4-digit
	Formula:	R4CZ ti Tschrh. (Russian 4-digit code enciphered by substitution sequences).
	Structure:	4-digt code of 35 pages with 100 Positions each (3500 positions in all), alphabetic-terminologic sequence. Alphabet, bigrams, trigrams, syllables, words, 2-digit numbers, punctuation and a number of reserve cells for optional entries.
	Encipherment:	Dinome substitution (substitution sequences or tables) for elements AB and CD.
	Area of use:	Used occassionally as emergency system by almost all NKVD organizations.
	Message content:	Very varied, sometimes tactical touching on army matters. Content often very important and interesting.
	Period of use:	August 1938 to January 1943
	Predecessor:	None
	Successor:	The 4-digit codes of the various NKVD organizations.
	Traffic receipts:	Very varied. Sometimes (for months at a time) no receipts, sometimes very heavy receipts.
	Readability:	After recovery in 1938/39 homogeneous material of at least 300 groups completely readable.
	Remarks:	This system was in use longer than any other military or political system of the USSR.

17.	Original designation:	Unknown
	General designation:	Second code of the NKVD border guard troops Kasakastan.
	Message groups:	4-digit
	Formula:	R4CZ. ü. Tschrh. (Russian 4-digit code enciphered by substitution sequences).
	Structure:	4-digit code of 50 pages with 100 positions each (5000 positions in all), otherwise like 16.
	Encipherment:	Like 16.
	Area of use:	NKVD border guard troops Kasakstan
	Message content:	General border guard matters and press reports.
	Period of use:	March 1937 to March 1939
	Predecessor:	First code of border guard troops Kasakstan (see 9).
	Successor:	First general code of NKVD border guard troops (see 18)
	Traffic receipts:	Seasonal, very heavy in summer, often up to 20 messages a day.
	Readability:	Like 16.
	Remarks:	None
18.	Original desingation:	Unknown
	General designation:	First general code of NKVD border guard and security troops.
	Message group:	4-digit
	Formula:	R4CZ. ü. Tschrh. (Russian 4-digit code enciphered by substitution sequences.
	Structure:	4-digit code of 100 pages with 100 positions each (10,000 positions in all), otherwise like 16 but considerably expanded, but many reserve cells for entering proper names.

	Encipherment:	Monogram phase substitution (3 phases); since April 1940 by additive sequence produced from the book "History of Leninism".
	Area of use:	All border guard districts of NKVD border guard and security troops.
	Message content:	General border guard affairs.
	Period of use:	March 1939 to December 1941
	Predecessor:	The general border guard Cäsars of the various border and coast guard districts and the second code of border guard troops Kasakstan.
	Successor:	The second general code (non-alphabetic) of the NKVD border guard and security troops.
	Traffic receipts:	Very heavy. Messages from all districts often up to 100 a day.
	Readability:	As for 16.
	Remarks:	None
19.	Original designation:	Unknown
	General designation:	First general tactical code of army and airforce.
	Message groups:	4-digit
	Formula:	R4ZC. ü Tschrh. (Russian 4-digit code enciphered by substitution sequences).
	Structure:	4-digit code of 50 pages with 92 positions each (4600 positions in all). Otherwise like 16 but adapted to needs of army and air force.
	Encipherment:	Like 16.
	Area of use:	Army and airforce generally. Corps, division, brigade and regiment.
	Message content:	Mostly tactical
	Period of use:	June 1937 to June 1939

	Predecessor:	Various small codes of short life and limited areas, also the first army code in the military district of Moscow (see 15), and the second general airforce code "VAK-38" (see 14).
	Successor:	"OKK-5" (see 20)
	Traffic receipts:	Very heavy during manoeuvers, otherwise light.
	Readability:	As for 16.
	Remarks:	None
20.	Original designation:	"OKK-5" (general commander code)
	General designation:	Second general tactical code of army and airforce.
	Message group:	4-digit
	Formula:	R4ZC. ü. Tschrh (Russian 4-digit code enciphered by substitution sequences)
	Structure	4-digit codes of 60 pages, 100 positions each (5000 positions in all), otherwise like 16 or 19, considerably improved and expanded.
	Encipherment:	Like 16.
	Area of use:	Like 19.
	Message content:	See 19.
	Period of use:	June 1939 to June 1940
	Predecessor:	First general tactical code of army and airforce (see 19)
	Successor:	"OKK-6" (see 21)
	Traffic receipt:	As for 19.
	Readability:	As for 19
	Remarks	None
21	Original designation:	"OKK-6" (General commander code).
	General designation:	Third tactical code of army and airforce.

	Message groups:	4-digit
	Formula	R4ZC d. Tschrh. (Russian 4-digit code enciphered by substitution sequences)
	Structure:	Like 20, further improved
	Encipherment:	Like 16
	Area of use:	Like 19
	Message content:	Like 19
	Period of use:	June 1940 to September 1941.
	Predecessor:	"OKK-5" (see 20)
	Successor:	"OKK-7" (see appendix 22--2).
	Traffic receipts:	As for 19
	Readability:	As for 16.
	Remarks:	None
22.	Original designation:	Unknown
	General designation:	First operational and tactical code of the supreme command of the RKKA for army and airforce.
	Message groups:	5-digit
	Formula:	R5ZC. m. Wurmdb (Russia 5-digit code with additive encipherment).
	Area of use:	Army and airforce. General staff down to division.
	Message content:	Tactical and operational (invasion of Poland and war with Finland.)
	Structure:	5-digit code with some 15000 positions in alphabetic-terminologic sequence. Alphabet, bigrams, trigrams, syllables, words, compound concepts, phrases, punctuation, fractions and ordinals, numbers from 0 to 1000, hours and minutes, day dates, year dates and caliber designations.

Encipherment:	Additive, primarily "general additive" (see part 2,
Period of use:	August 1939 to December 1940
Predecessor:	Unknown, probably no such system had been used before.
Successor:	"011--A" (see 22)
Traffic receipts:	Very heavy during the Russo-Finnish war.
Readability:	When the same additive was reused (at least 3 messages, preferably more) this was read in part, later quite completely.
Remarks:	None

23. Original designation: "011-A"

General designation:	2nd operational and tactical code of the supreme command of the RKKA for army and airforce.
Message group:	5-digit
Formula:	R5CZ. m. Wurmlb. (Russian 5-digit code with additive encipherment).
Structure:	5-digit code of 390 pages and some 19000 positions. Otherwise like 22. Considerably improved among other things with numerical designations for army, corps, divisions, and brigades.
Encipherment:	Like 22
Period of use:	January 1941 to October 1941
Area of use:	Army and airforce. General staff down to regiment.
Message content:	Tactical and operational (Russo-German war).
Predecessor:	First operational and tactical code of the supreme command of the RKKA for army and airforce. (see 22)
Successor:	"023-A" (see appendix 22 - 5.)
Traffic receipts:	Very heavy, up to 300 messages a day on the average.

Readability: As for 22. Due to increased use of "individual additive sequences" and frequent change of "general additive sequences" the percentage of readability was between 15 and 25%.

Remarks: "Oll-A" was captured in June 1941

For continuation: See appendix 22.

Appendix 22

Compilation of the most important systems of the army, airforce, and NKVD during the Russo-German war 1941/45 which were decrypted and captured.

1. Original designation:	"PT--41" (chatter table for 1941).
General designation:	3rd general operational system of army and airforce.
Message groups:	2-digit (sometimes sent as 4-digit groups.)
Formula:	R2CZr. m. dop. Lsart. (Russian 2-digit Cäsar with double reading).
Structure:	2-digit Cäsar with 198 positions. Alphabet, digits and most important punctuation marks have two values. Most frequent letters have three. Improved selection of words for operational and communications technique and a few tactical words. 2 switch groups ("read letters" and "read words"), to care for the double entries.
Encipherment:	System squares for single digit substitution of tens and units.
Area of use:	Army and airforce generally, from division down, as emergency system also for army.
Message content:	Predominently operational, internal service and personnel matters. As emergency system also tactical content.
Period of use:	March 1942 to the end of 1943, sporadically down to the beginning of 1944.
Predecessor:	"PT--39" (compare appendix 21 -- 2).
Successor:	Various "SUV" and "PT" systems used in small areas.
Traffic receipts:	Heavy in the beginning.
Readability:	Homogeneous material of at least 100 groups completely readable.
Remarks:	Captured during the early months of the war, almost completely recovered and readable before that.

2. Original designation:	"OKK-7" (general commander code).
General desingation:	4th general tactical code of army and airforce.
Message groups:	4 digit.
Formula:	R4ZC ü. Tschrh. (Russian 4-digit code enciphered by substitution sequences).
Structure:	4-digit codes of 50 pages with 100 positions each. Alphabetic-terminologic sequence. Alphabet, bigrams, trigrams, syllables, words, 2-digit numbers, punctuation marks, several compound tactical concepts and cover groups, also reserve groups.
Encipherment:	Dinome substitution (substitution sequences or tables) for elements AB and CD, sometimes with the use of indicator groups.
Area of use:	Army and airforce in general. Army, corps, division, brigade and regiment.
Message content:	Chiefly tactical.
Period of use:	November 1941 to January 1942.
Predecessor:	"OKK—6" (see appendix 21 -- 21.)
Successor:	"OKK—8" (see 3)
Traffic receipts:	Unstable, varied from net to net, 50 messages a day on the average.
Readability:	After capture homogeneous material of at least 300 groups completely readable, prior to that fragments could be read.
Remarks:	The code was captured a few days after it was put into use, however the encipherment always had to be broken.
3. Original designation:	"OKK-8", (general commander code)
General designation:	5th general tactical code of army and airforce.
Message groups:	4-digit
Formula:	R4ZC ü. Tschrh. (Russian 4-digit code enciphered by substitution sequences).

Structure:	Like 2, further improved.
Encipherment:	Like 2.
Area of use:	Like 2.
Message content:	Like 2.
Period of use:	January 1942 to March 1942.
Predecessor:	"OKK—7" (see 2)
Successor:	No 4—digit code of this type was in use after the reorganization of the cryptographic service of the RKKA in March 1942.
Traffic receipts:	As under 2, constantly diminishing.
Readability:	As for 2.
Remarks:	As for 2.

4. Original designation: "OZKK—7" (central commander code)

General designation:	First central tactical code of units of the RKKA not in the front (supply area or training area).
Message groups:	4-digit
Formula:	R4ZC. u. Tschrh. (Russian 4-digit code enciphered by substitution sequences).
Structure:	Like 2.
Encipherment:	Like 2.
Area of use:	Units of the RKKA from army down to regiment in the supply or training areas.
Message content:	Organization, supply, personnel etc., also tactical.
Period of use:	July 1941 to March 1942
Predecessor:	Unknown, probably none.
Successor:	Various SUV systems.
Traffic receipts:	Sometimes heavy.
readability:	As for 2.

Remarks:	Completely readable from the start since both code and key tables had been captured complete.
5. Original designation:	"023—A"
General designation:	3rd operational and tactical code of the supreme command of the RKKA for army and airforce.
Message groups:	5-digit
Formula:	R5ZC. m. Wurmdb (Russian 5-digit code with additive encipherment).
Structure:	5-digit code with 20,000 positions in alphabetic—terminologic sequence. Alphabet, bigrams, trigrams, syllables, words, compound concepts, phrases, punctuation marks, fractions and ordinals, numbers from 0 to 1000, hours and minutes, day dates, year dates, calliber designations and numerical designations of armies, corps, divisions, brigades, and some mixed units.
Encipherment:	Additive—"general"and "individual" bloknots. (compare part 2 pages 90/91)
Area of use:	Army and airforce. General staff down to division and brigade.
Message content:	Tactical and operational. (Russo-German war)
Period of use:	October 1941 to March 1942
Predecessor:	"011—A" (see appendix 21—23).
Successor:	"045—A" (see 6)
Traffic receipts:	Very heavy, all told up to 300 messages a day.
Readability:	Good where the same sequence was reused, (at least three messages, preferably more). Increased use of "individual bloknots", sometimes contrary to regulations used several times and consequently read. Often as many as 60 messages a day, i. e. 20%.
Remarks:	The code was captured immediately after it was put into use.

6.Original designation:	"045—A"
General designation:	4th operational and tactical code of the supreme command of the RKKA.
Message groups:	5-digit
Formula:	R5CZ. m. Nurmüb. (Russian 5-digit code with additive encipherment).
Structure:	5-digit code with 21,000 positions. Otherwise like 5 but further expanded and improved. Interrupted alphabetic sequence.
Encipherment:	Like 5.
Area of use:	Like 5.
Message content:	Like 5.
Period of use:	March 1942 to March 1943.
Predecessor:	"023-A" (see 5)
Successor:	"062-A" (see 7)
Traffic receipts:	Like 5
Readability:	Like 5 but with increased, correct use of "individual" additive. Readability decreasing.
Remarks:	Code was not captured until summer, by then it was so far broken that fragments could be read and the general sense gleaned.
7.Original designation:	"062—A"
General designation:	5th operational and tactical code of the supreme command of the RKKA for army and airforce.
Message group:	5-digit
Formula:	R5CZ. m. Nurmüb (Russian 5-digit code with additive encipherment).
Structure:	5-digit code with 22,000 positions. Alphabetic-terminologic sequence. Like 5 but further improved and expanded.

Encipherment: Like 5.

Area of use: Like 5.

Message content: Like 5.

Period of use: March 1943 to March 1944.

Predecessor: "045—A" (see 6)

Successor: "091—A" (see 8)

Traffic receipts: Like 5.

Readability: Like 6

Remarks: Code was captured immediately after it was put into use.

8. Original designation: "091—A"

General designation: 6th operational and tactical code of the supreme command of the RKKA for army and airforce.

Message groups: 5-digit.

Formula: R5ZC. m. Wurmdb . (Russian 5-digit code with additive encipherment)

Structure: 5-digit code with 23000 Positions in alphabetic-terminologic sequence. Comma and period with multiple values, generally once on each page. For the rest like 5.

Encipherment: Like 5.

Area of use: Like 5.

Message content: Like 5.

Period of use: March 1944 to May 1945 and probably longer.

Predecessor: "062—A" (see 7)

Successor: not known.

Traffic receipts: Like 5.

Readability: Ever decreasing. Rare use of "general" additive, disguise of indicator groups.

Remarks:	Code captured shortly after it was put into use.
9. Original designation:	Unknown.
General designation:	First non-alphabetic code of interior troops NKVD and of border guard and security troops (front staff and GUP) facing hostile countries.
Message groups:	4-digit
Formula:	RAZC. m. Nurmib Russian (4-digit code with additive encipherment)
Structure:	4-digit code with 100 pages of 100 positions each (10,000 positions). Non-alphabetic sequence. Alphabetic, bigrams, trigrams, syllables, words, compound concepts, numbers from 0 to 100, marks of punctuation and reserve cells.
Encipherment:	Additive table (so called Gamma tables) For a time in the arctic district transposition with numerical key.
Area of use:	Internal troops NKVD. Highest command of border guard and security troops NKVD facing enemy countries.
Message content:	Organization, administration, internal service, political training, security measures within the forces, special schooling, defense (Abwehr) execution of sentences. Occasionally tactical.
Period of use:	January 1942 to October 1944.
Predecessor:	First general code of NKVD border guard and security troops (see Appendix 21 — 18.)
Successor:	Second non-alphabetic code of interior troops NKVD and the border guard and security troops facing enemy countries. (see 10)
Traffic receipts:	Heavy, constantly increasing. Up to 300 messages daily.
Readability:	Very good due to frequent use of the same additive. Recovery of the code was very laborious, only fragments could be read down to the end of 1942.
Remarks:	None

10.	Original designation:	Unknown
	General designation:	Second non-alphabetic code of interior troops NKVD and of border guard and security troops facing hostile countries. (front staff and GUP)
	Message groups:	4-digit.
	Formula:	RAZC. m. Warmüb (Russian 4-digit code with additive encipherment).
	Structure:	Like 9, but improved.
	Encipherment:	Only additive. Since January 1945 double additive for (gamma tables).
	Area of use:	Like 9
	Message content:	Like 9
	Period of use:	October 1944 to May 1945 and apparently later.
	Predecessor:	First non-alphabetic code of interior troops NKVD and for border guard and security troops facing enemy countries. (front staff and GUP) (see 9)
	Successor:	Not known.
	Traffic receipts:	Like 9, often more than 300 messages a day.
	Readability:	After recovery of the code consistently good in spite of double additive encipherment which was almost always incorrect.
	Remarks:	It is quite possible that this system is still in use. (Autumn 1947).
11.	Original designation:	Unknown
	General designation:	First non-alphabetic code of NKVD border guard and security troops facing neutral countries. Kasakstan, Outer Mongolia and Manchuria (Far East), all units.
	Message groups:	4-digit.

Formula:	R4CZ. m. Nurmlb. (Russian 4-digit code with additive encipherment).
Structure:	Like 9
Encipherment:	Additive sequence. Originally produced from a book "Signal Service", later additive using couplings of digit sequences.
Area of use:	All units of the border guard and security troops facing neutral countries. Kasakstan, Outer-Mongola, Manchuria, and the Far East.
Message Content:	Like 9 but not tactical. Administration and control of prisoner of war camps, penal units and concentration camps.
Period of use:	September 1943 to May 1945, and apparently later.
Predecessor:	Unknown, possibly first general code of NKVD border guard and security troops. (see appendix 21—18).
Successor:	Not known
Traffic receipts:	Varied, sometimes up to 50 messages a day. Probably inadequately monitored.
Readability:	Good since the same additive was often reused.
Remarks:	None
12.Original designation:	Unknown
General designation:	Code table of railway troops NKVD.
Message groups:	5-digit
Formula:	R5ZC. ü. Tschrh. (Russian 5-digit code enciphered by substitution sequences).
Structure:	5-digit code of 25 pages. Each page divided into 4 quarters, each quarter with 25 positions (2500 positions all told). Alphabetic-terminologic sequence. Alphabet, bigrams, trigrams, syllables, words, numbers from 0 to 100, punctuation marks.

Encipherment:	Dinome substitution for elements AB and DE, single digit substitution of element C.
Area of use:	Railway troops NKVD.
Message content:	Communication system supplies, safeguarding transports, guarding important and endangered stretches and points.
Period of use:	1943 to May 1945 and beyond.
Predecessor:	Unknown
Successor:	Not known.
Traffic receipts:	In 1943/44 often very heavy, later lighter.
Readability:	After recovery of the system completely readable when homogeneous material of at least 150 groups was available.
Remarks:	None

13. Original designation: "SERNO"

General designation:	First code table of forward units of NKVD border guard and security troops.
Message groups:	4-digit
Formula	R4CZ. ü. Tschrh. (Russian 4-digit code enciphered by substitution sequences).
Structure:	4-digit codes with 50 pages of 50 positions each, 2500 positions. Alphabetic-terminologic sequence. Alphabet, bigrams, trigrams, syllables, words, numbers from 0 to 31, punctuation marks, reserve cells, and cover groups. On each network a large number of family names of military and political leaders were included.
Encipherment:	Dinome substitution sequences for elements AB and CD, different for each net.
Area of use:	Border guard and security troops NKVD front staff to battalion.
Message content:	Border service, security service, counter-espionage, removal and resettlement of population, customs and police functions, work on fortifications and road building, supply.

Period of use:	1943 to May 1945
Predecessor:	None, a supplementary system for lower formations,
Successor:	Was to be replaced by code table "NIVA" but continued in use after NIVA appeared.
Traffic receipts:	Very heavy, up to 200 messages a day. Not completely intercepted.
Readability:	Very good when enough traffic was received from an individual net. Up to 100 messages a day could be read.
Remarks:	None.

14. Original designation: "NIVA"

General designation:	Second code table of forward units of NKVD border guard and security troops.
Message groups:	4-digit
Formula:	R4CZ. U. Tschrh. (Russian 4-digit code enciphered by substitution sequence).
Structure:	4-digit code of 21 pages of 50 positions each (2100 positions), for the rest like 13.
Encipherment:	Like 13.
Area of use:	Like 13.
Message content:	Like 13.
Period of use:	February 1945 to May 1945 and beyond.
Predecessor:	To some extent "SERNO"
Successor:	Not known
Traffic receipts:	Like 13
Readability:	Like 13
Remarks:	It is quite possible that this system is still in use (autumn 1947).

15. Original designation:	"VISA"
General designation:	Code table of the lowest units of NKVD border guard and security troops. Formula R4CZ. gem. Tausch (Russian 4-digit code with mixed substitution).
Structure:	4-digit code of 20 pages with 50 positions each. (2000 positions). Partly alphabetic; tactical designations, proper names entered alphabetically in a separate part. Numbers from 0 to 99. Otherwise like 13.
Encipherment:	Dinome substitution for elements AB, single digit substitutions for elements C and D.
Area of use:	Border guard and security troops NKVD from regiment down to outposts and individual groups.
Message content:	Like 13.
Period of use:	1943 to May 1945
Predecessor:	None, additional system for the lower echelons.
Successor:	Not known.
Traffic receipts:	Up to 50 messages a day, at times considerably less.
Readability:	Like 13
Remarks:	None
16. Original designation:	"SUV" (Camouflaged communications of the top command)
General designation:	All minor and medium systems used for a short time and in limited areas which exceeded the limits of the Cäsar.
Message groups:	3, 4 and even 5-digit, sometimes mixed numbers.
Formula:	Various R3, 4 or 5ZC. (Russian 3, 4 and even 5 digit codes).
Structure:	3, 4 and 5 digit codes, tables and signal tables. Between 500 and 2000 positions. Alphabetic and interrupted alphabetic sequence. In rare cases non-alphabetic. Alphabet, syllables and short words as well as a selection of

	words important to the units concerned. Usually only digits. Lately often without alphabet, with two or more switch groups signifying "read the first letter of the word" or "read the entire word".
Encipherment:	Dinome and monome substitution in the most varied combinations.
Area of use:	Army and airforce. Army down to the company. Airforce down to the ground organization.
Message content:	Tactical, sometimes also operational.
Period of use:	In the army the single systems were always shorter lived than those of the airforce which were usually more extensive. Generally varied from one week to a half year.
Predecessor:	Various relatively long term systems for general use of the army and airforce.
Successor:	Not known.
Traffic receipts:	Very heavy, up to 500 messages a day.
Readability:	Varied, depending on length of use and the amount of homogeneous material.
Remarks:	none.
17. Original designation:	"PT" (chatter tables)
General designation:	Cäsars and very small codes.
Message groups:	2, 3 and 4-digit.
Formula:	R2, 3 or 4 ZCr. and ZC. (Russian 2, 3, or 4-digit Cäsar or code).
Structure:	2, 3 or 4-digit Cäsars or 3, and 4 digit codes. Alphabetic, interrupted-alphabetic and also non-alphabetic sequence. Usually alphabet, short words, digits 0 to 9, punctuation and some selected words.
Encipherment:	As for 16.
Area of use:	Army and airforce, from the division down.

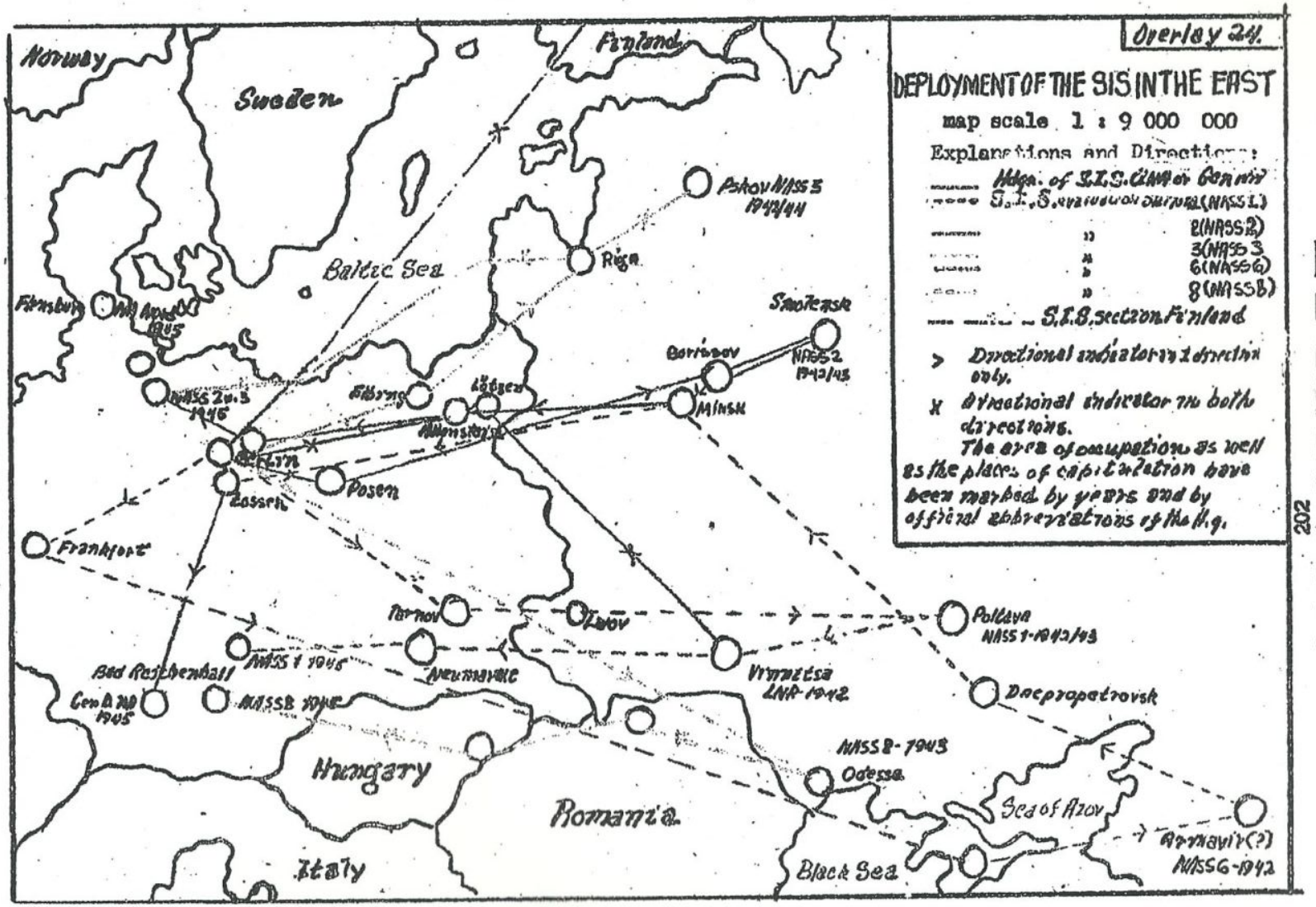
Message content:	Operational and communications technique, internal service; organization, training, personnel matters, and -- as emergency system -- also tactical.
Period of use:	Generally brief, 1 week to 1 month.
Predecessor:	"PT-41" (see appendix 21--1.)
Successor:	Not known
Traffic receipts:	Varied, generally heavy, up to 100 messages a day.
Readability:	Like 16.
Remarks:	None.

Overlay 23

Comparative Transcription

Russian Alphabet	Equivalent in the Roman Alphabet in Morse Code.	Phonetik transcription of the Russian words. English	German
А,а	a	a	a
Б,б	b	b	b
В,в	w	v	w
Г,г	g	g	g
Д,д	d	d	d
Е,е,Э,э	e	e, ye	e, je
Ж,ж	v	j	sh
З,з	z	z	s
И,и	i	i	i
-,й	j	y	j
К,к	k	k	k
Л,л	l	l	l
М,м	m	m	m
Н,н	n	n	n
О,о	o	o	o
П,п	p	p	p
Р,р	r	r	r
С,с	s	s	ss, s
Т,т	t	t	t
У,у	u	u	u
Ф,ф	f	f	f
Х,х	h	kh	ch, h
Ц,ц	c	ts	c, z
Ч,ч	ö	tch	tsch
Ш,ш	ch	ch	sch
Щ,щ	q	shch	schtsch
-,ы	y	i	y
-,ь	x		(j)
Ю,ю	ü	u, yu	ju
Я,я	ä	ya	ja

TOP SECRET



TOP SECRET

APPENDIX 25

TABLE SHOWING ACCOMPLISHMENTS & PERSONNEL STRENGTH OF THE FIXED INTERCEPT STATION AT JUTERBOG (TREUENBRIETZEN) TOGETHER WITH ITS OUT STATIONS 1935 to 1939. (IN ROUND NUMBERS)

- ASSIGNMENT: RUSSIA AND POLAND -

Period	Out-stations	Number of Re-ceivers	Number of economic and diplomatic messages intercepted monthly for Berlin	RUSSIA Army, airforce and NKVD		POLAND Army, airforce, border-guard.		Personnel strength of the Cryptanalytic Section	
				Number of messages intercepted a month	Number of messages deciphered a month	Number of intercepts a month	Number of messages deciphered a Month	Russia	Poland
3.4. 35	-	7	1500	250	100	500	150	1	2
5.35-10.35	Pasewalk Schlochau Schneide-mühl	20	2500	400	150	1000	200	1	2
10.35-3.36	"	20	3500	600	200	1000	200	4	3
3.36-3.37	Pasewalk Schlochau Schneide-mühl Fraustadt Meseritz	30	4000	800	250	1200	250	5	4
3.37-4.38	"	30	3000	1500	400	1500	300	7	5
3.38-4.39	"	30	2000	2500	750	1500	300	9	5

TOP SECRET

TOP SECRET

TOP SECRET

APPENDIX 26

COMPARISON OF PERSONNEL STRENGTH OF THE RUSSIAN SECTION

WITH ACCOMPLISHMENTS (1939--1945) (IN ROUND NUMBERS, ESTIMATED).

Year	Personnel Strength:								Number of messages read (deciphered) a month	Percentage of duplicated decipherment a month
	H.-Leitstelle, L. N.A., Gen. d. Nachr.-Aufkl.	NAAS 1 "Süd"	NAAS 2 "Mitte"	NAAS 3 "Nord"	NAAS 6 Caucasus from 43 on Partisan bands	NAAS 8 "Südukraine"	Nachr. - Abtlg. "Finnland"	Total		
1939	25	-	-	-	-	-	-	25	2000	up to 5%
1940	40	-	10	-	-	-	-	50	3000	about 10%
1941	60	10	20	10	-	-	10	110	5000	about 25%
1942	80	20	30	20	20	20	15	205	7000	about 30%
1943	100	30	40	30	30	25	20	275	8000	up to 40%
1944	70	25	30	25	25	25	15	215	7000	about 35%
1945	50	20	30	-	-	20	-	120	5000	up to 25%

TOP SECRET

Cryptanalytic aids and methods particularly for Russian cryptograms.

I. Preface and introduction.

II. Cryptographic Aids

A. Results of linguistic study

1. Letter frequencies
2. Frequencies of genuine and spurious bigrams.
3. Frequencies of genuine and spurious trigrams.
4. Word frequencies.
5. Short words in Russian.
6. Linguistic peculiarities, such as intervals between letters, double letters, and frequent groupings of letters.
7. Miscellaneous.

B. Results of studies of the text of Russian military and political cipher messages.

1. The vocabulary of military-political cryptograms.
2. General remarks on telegraphic style.
3. Textual weaknesses as entry points for breaking.

a. Punctuation marks
b. Family names, and patronimics.
c. Address and signature.
d. Place names
e. Troop movements
f. Time and date
g. Coordinates
h. Stereotyped reports
i. Enumerations
k. Abbreviations.

C. General aids.

1. Forms, counts and card indices
2. Bibliography and map material.
3. Preliminary study, sorting and logging of enciphered radiograms.
4. Hollerith procedure as crypt analytic aid.
5. Mechanical aids.

III. Methods of decryption.

A. General methods.

1. Studies to determine the system.
2. Frequency count.
3. Indexing.
4. Repetitions and parallel passages.
5. Compromises and partial compromises.
6. Simple and expanded search for vowels and consonants.
7. Recovery of [key] words from numerical keys.

B. Practical decryption of simple and combined substitution systems.

1. The Cäsar and its variants.
2. Code and Satzbuch.
   a. Alphabetic arrangement.
   b. Non-alphabetic arrangement.
3. Encipherments.
   a. Substitution system.
   b. Numerical sequence and additive sequence.

C. Practical decryption of simple and combined transposition systems.

1. The transposition (Wärfel) and its variants.
2. Double transposition.
3. The grille (The Raster).
   a. Revolving grille
   b. The ordinary (usual) grille

D. Practical decryption of systems combining substitution and transposition.

IV. Conclusion

(Slight alterations in arrangement may be made.)

[an outline only—no text]

Problems of cryptanalysis.

(In particular of Russian military and political cryptograms)

Preface

Part 1: Cryptography

A. Introduction
B. History of cryptography
   1. Antiquity
   2. Middle ages
   3. Modern times
C. Present day cryptographic systems.
   1. Hand and memory systems.
      a. Substitution
      b. Transposition
      c. Combined systems.
   2. Machine ciphers.
D. Cryptanalysis within the framework of signal intelligence
   1. The assignment
   2. Personnel strength
   3. Looking back and looking ahead.

Part 2: Cryptographic aids

A. Maintenance of secrecy.

B. General aids
   1. Literature, special papers, and map material.
   2. Forms
      a. The intercept message form.
      b. Forms for letter count and for decrypted systems.
   3. Sorting, logging and preliminary study of cipher messages.
   4. Hollerith methods and mechanical aids.
   5. Card catalogues.

C. Results of linguistic study.
   1. Letter frequencies
   2. Frequency of genuine and spurious bigrams
   3. Frequency of genuine and spurious trigrams.
   4. Word frequencies.
   5. Short words in Russian
   6. Linguistic peculiarities such as double letters, letter intervals and frequent groups of letters.
   7. Miscellaneous.

D. Results of textual study of the Russian military and political cryptograms.

1. The vocabulary.
2. General remarks on telegraphic style.
3. Textual weaknesses as points of analytic entry.
   a. Marks of punctuation
   b. Family names and patronimics
   c. Address and signature
   d. Place names
   e. Troop movements
   f. Time and date
   g. Coordinates
   h. Sterotyped reports
   i. Immumerations
   k. Abbreviations

Part 3: Methods of decipherment:

A. General methods.

1. Studies to determine the system.
2. Frequency counts.
3. Indexing (groups)
4. Repetitions and parallel passages.
5. Compromises and partial compromises.
6. Simple and expanded search for vowels and consonants.
7. Recovery of [key] words from numerical keys.

B. Practical decipherment of simple and combined substitution systems.

1. The Cäsar

   a. The simple Cäsar
   b. The expanded Cäsar
   c. The Cäsar with variants
   d. Spaltencäsar (polyalphabetic substitution)

2. Code and Satzbuch

   a. In alphabetic sequence [1 part]
   b. In non-alphabetic sequence [2 part] Chiffrant and Dechiffrant).

3. Encipherments
   a. Substitution system
   b. Digit sequence and additive sequence.

C. Practical decipherment of simple and combined transposition systems.

1. The Würfel

a. Single transposition and its variants.
b. The Diagonalwürfel.
c. Double transposition.

2. The Raster (grille)

a. The revolving grille.
b. The ordinary Raster.

D. Practical decipherment of systems combining substitution and transposition.

1. Double encipherments

2. Multiple encipherments.

[This appears to be a second outline--Text of Part 2,Section B follows — no other text received.]

B. Cryptographic aids

1. General aids. In the class of general aids fall all those aids which as a rule have been thought up by individual workers in the course of their cryptanalytic activities, have been tried out and found generally useful. The same collective name is also applied to literature on the subject and to the requisite map material. During many years of practical work as a result of experience and of the development of cryptology as a whole, the term general aid has been expanded to include not merely the tools of the cryptanalyst but all those manipulations which may be regarded as preliminary steps although they are not a part of the actual decipherment. In a broad sense the handling of incoming cipher messages, i. e. logging, sorting and preliminary study and the resulting treatment by Hollerith methods, where practicable, head the list of such general aids. As last of these general aids we may mention mechanical aids whose importance, as will be seen later, is often problematic and which with their often superfluous complexity are likely to intrigue the layman although only in rare cases do they produce results which justify the outlay of money and time involved.

1. Literature, special papers, and map material.

"Divide et impera" in the field of security applies also to the handling of the literature and map material within the framework of cryptanalysis and content evaluation. All reference books and all published documents are accessible to all workers as a matter of course.

The analytic and evaluation sections however will possess a more or less extensive collection of printed or written material, depending on the size of the section, i. e. the field covered and the time it has been in existance, such material belonging to all possible security classifications. Before discussing this classified material however attention may be called to the necessary literature available to all.

First and most used are all reference works such as dictionaries, Dudens [orthographic dictionaries] , encyclopedias and atlases, also simple map material.

In detail:

1. Simple two language dictionaries.
2. Two language military dictionaries.
3. Two language technical dictionaries.
4. Duden in the mother tongue.
5. Duden in the language of the country concerned.
6. Encyclopedias, including military encyclopedias if possible, both in the mother tongue and the language of the countries concerned.
7. Atlases and alphabetic gazateers.
8. Simple map material of the country studied in single sheets

a. For general orientation (scale 1: 1 000 000 to 1: 10 000 000).

b. For airforce and navy (scale 1: 300 000)

c. For the army (scale 1: 50 000 to 1: 100 000, for thickly settled or industrial areas 1: 25 000)

The analytic and evaluation sections also need all books, newspapers, periodicals and writings which throw light on the official status of the country in question in respect to its policies, military power, technology and economic life.

These include:

1. Newsapers of the country, military, political, technical, economic publications, weeklies, monthlies, and special papers.

2. Books like Passow's "Frende Heere" or Weyer's "Taschenbuch der Kriegsflotten" and "Jahrbuch der Luftfahrt" or Gröner's "Taschenbuch der Handelsmarinen" etc.

The value of these published works is very problematic as far as the USSR is concerned. It must not be forgotten that this complex of states has endeavored since 1917/18 to reveal to the outside world as little as possible of its internal life, that the concept of the "Iron Curtain" is not new and that even in relatively quist times it was extremely difficult to obtain any exact information and so to publish anything even approximately corresponding to the facts. This sphinx-like conduct of Bolshevist Russia applies also to its own people, in this connection it may be mentioned that Russian carrography before the change from verst to kilometer maps, i. e. down to 1937, did not meet the most primative requirements and also that maps were not on sale to the general public. The old verst maps, usually of English origin, and land surveys were quite out of date and suffered from poor phonetic reproduction of names as well as for the constant renaming of places. Although after the reform things were

materially better in this respect in Russia itself, it was practically impossible to secure new maps of the USSR. In order to be independent of these, maps of the USSR extending as far as the Moscow area on the scale 1: 100 000 and 1: 300 000 were printed in Germany by order of the General Staff. Old maps and a few new Russian maps 1: 300 000 and 1: 500 000 which could be gotten across the frontier served as the basis for these maps. Of course the chronic Russian disease of constantly changing place names was taken into account as far as possible. In Germany these maps were given the lowest classification "only for official use" but were among the most used aids in the analytic and evaluation sections of the former German signal intelligence and had to be available to all workers.

To supplement the maps, primarily for current correction of place names, an attempt was made in 1936 to procure a complete Russian railway timetable through the publisher Ascher after an attempt to secure these books from "Intourist" in Berlin had failed. By liberal expenditure of time and money it was possible to secure one copy in each of the years 1936—1938. This example will serve to demonstrate the difficulty of getting pertinent documents.

The following literature or in some cases cryptographic aids created by ourselves using Hollerith machines, were classified "only for official use". They are mainly concerned with Russia.

1. An alphabetic list of Russian family names (Based on the Moscow city directory).

2. The same names read backward, in alphabetic sequence (Hollerith).

3. A gazateer read backwards, in alphabetic sequence (Hollerith).

4. Various books on methods of solving cross-word and syllable puzzles in German, English, French and Russian.

5. Published works on cryptanalysis.

6. A compilation of formulae covering the binominal theorem, thsory of series, and theory of probability.

7. All literature on mathematical analysis.

8. Intercepted cipher messages which had not been worked on.

9. A list of Russian post offices, telegraph agencies and radio transmitters.

One should not be surprised to find that part of the material classified by signal intelligence as "only for official use" is actually published material. It must be obvious however that the sum of such literature points to the special field of endeavor and therefore must at least be kept under lock and key.

In the next category "secret" belong a large number of documents which, following the rule "divide and conquer" need not be accessible to all workers. The question of security in respect to these documents must be treated differently from case to case, basic regulations are hardly applicable, each administrative head must be allowed to use his own judgement.

To avoid mistakes however it must be said that a certain latitude must be allowed all the principal workers both in cryptanalysis and evaluation, since otherwise delays may occur and initiative, industry and zeal be checked.

The following are classed as "secret":

1. All signal intelligence bulletins, all reports, compilations and commentaries resulting from evaluation of press and radio broadcasts (in Germany these reports during the war were classified "Top Secret", they were designated as "Chi-Nachrichten" because they were issued by the cipher sections of OKW and were accessible only to a very limited circle).

2. "VN — Meldungen" (Verläszliche Nachrichten), i. e. compilations of deciphered and translated cipher messages. (Without indication that they were deciphered!)

3. "Die Feindlage" (Red Situation Map without commentary).

4. All map material showing entry of troop movements based on signal intelligence.

5. Tables and papers dealing with analysis of language and text.

6. Compilations of military and political terms from deciphered cryptograms.

7. Results and reports of traffic analysis.

8. Lists of Russian abbreviations.

9. All card files of evaluation results including files of names, troop units, abbreviations, plane types, weapons and equipment, factories, etc.

10. All working material such as blank forms and file cards.

All secret material was supposed to be kept in steel safes, the card files were to be locked. In time of war, when a change of location becomes necessary or temporary quarters are used, strong wooden boxes with good locks and iron bands, better sheet-metal boxes ("Mobkisten"), are very necessary.

Papers of the highest classification, designated "Geheime Kommandosache" "Geheime Chefsache" or "streng geheim", were required to be kept in armoured safes.

In signal intelligence only the cryptanalytic and evaluation sections had to do with papers of this class and here an especially strict control of persons allowed to see such documents was to be exercised.

In the main the following were involved:

1. "Horchlage" (report of content evaluation). Evaluation results of all deciphered messages with commentary.
2. "Own situation" (Blue Situation Map) with commentary.
3. Commentary on the Red Situation Map.
4. Any material which would disclose decipherment directly or indirectly, including intercept forms with intermediate text and plaintext.
5. Reports on decipherment, achievement, experience and allocation of strength.
6. Descriptions of systems, codes, encipherments and captured documents.
7. Training material.
8. All unpublished literature on cryptanalysis.
9. Cryptographic files ("Steckbriefe").

This enumeration and breakdown of the literature falling under the heading "general cryptographic aids" does not pretend to be absolutely complete. No doubt the cryptanalytic unit of every country goes it own way in certain respects, moreover work on military-political material may be very different from that on enciphered economic and diplomatic messages. As stated in the introduction these observations are to be considered exclusively from the military-political standpoint.

2. Forms.

a. The intercept message form.

The most used and so perhaps the most important form for signal intelligence is the message blank which is filled in by the operator with the letters or the digits heard. This form, the "H. - Funkspruch" as it was called in the former German signal intelligence, never really served its purpose well although the ruling and format was changed repeatedly. The explanation may be found in the fact that the setting-up and revising of this form lay in the hands of persons who, although once mostly good operators and later useful conscientious traffic analysts, left out of account the principal purpose of the intercept form, namely its preliminary and final treatment by the cryptanalyst. Not that there was any lack of suggestions on the part of the cryptographic section, however the absolute disregard for this "abstract science" or "black art" as officers used to call it, and the general aversion to making it any concessions whatsoever, simply did not allow such suggestions to bear fruit. People forgot, and perhaps still forget, that the operator does not see the intercept form again after he has filled it out in a few minutes, that the traffic analyst, after he has noted a few details and compared them with existing records, likewise does not need the message any longer, but that the analyst has to work for hours, days or even weeks with this copy. Hence it would seem more than fair that the needs of the cryptographic section be given prime consideration when working out such forms.

Beyond a doubt the Finnish signal intelligence, small as it was in contrast to the German, showed more sense and objectivity in this respect among others. The message form shown in appendices 3 and 4 was suggested by the very practical example of the Finns

The demands to be made on such a form are very numerous because in the course of time more and more entries become necessary to meet the needs of the cryptographic and evaluation sections. These are listed below.

1. The operator must know where he is to enter the signals (letters or digits). In the old days this was left to the operator's own discretion. It happened sometimes that the operator for reasons of economy entered the cipher elements or groups line by line and practically no room was left for the decipherer to enter the plain-text and, as later became necessary, the intermediate text above the cipher elements.

   In the form (appendixes 3 and 4) the spaces provided for the operator's entries are clearly defined. In appendix 3 there are 6 wide lines, in appendix 4 ten wide lines divided by vertical lines to separate the groups. The form in appendix 3 is used for all radiograms and when a message exceeds 60 groups in length the form of appendix 4 is used as supplement. Hence appendix 4 is simply a supplement (or supplements) to that in appendix 3. It would be well to print the model of appendix 3 as face of the form sheet and that of appendix 4 as the back of the sheet.

   After the message groups have been entered the operator can easily compare their number with the group count in the message heading (or the letter count as the case may be), since with ten groups to the line a count is quickly and easily made. The form used in the former German signal intelligence service down to the time of capitulation had either 4 or 5 columns.

[4—5 groups to the line]

2. Before hearing the actual message the operator will make most of the entries in the heading.

H.—Einheit = intercept station.

Empfänger: = number of designation of the receiving instrument.

Nummer: = serial number assigned the message by the operator.

Funker: = name of the operator

Frequenz oder Welle: = frequency or wave band in meters or decimeters (1 entry suffices)

Lautstärke = signal strength, usually expressed by stages 1—4.

Remarks: may also be entered such as "poor operator", "static" "thunderstorm" or "jamming".

For future work the most important entries by the operator are the following:

von: = sending station (call sign with meaning if possible)

an: = addressee (call sign with meaning if possible)

am: = day date

um: = precise clock time, i. e. not merely the hour but the precise time in minutes.

message heading: = All data transmitted ahead of the actual message groups, including: operational signals, day date, tactical time (according to the standard of the country concerned), group count, possible key or indicator group, etc.

3. The item "Netz" (net) can be filled in by traffic analysis and this is best done by using abbreviations or formulae. If the traffic analyst puts a question mark after the net designation this means that the identification is not certain. It is best

to make this entry in pencil since it may have to be corrected or amplified when the message is worked on.

4. The heading "Verfahren" is for entry of the cryptographic designation by the cryptanalytic section. Here again it is best to use abbreviations.

5. The heading "Datum der Abgabe" is for fixing the time when the deciphered message is delivered to the evaluation section, it serves for control of the analytic section in general as well as of the individual worker.

6. The worker in the cryptanalytic section enters under the heading "Interne Nummer" his mark (initial or what not) and the serial number. These internal numbers run serially for each worker from the beginning to the end of the month (or for a 3 or 6 months period). The messages thus marked pass through the evaluation section and are then preserved in binders marked with the initial of the worker and the first and last number enclosed. In this way the whereabouts of any message can be checked — the serial numbers must all be there, and the accomplishments of each worker can be checked and finally every message can be quickly located if questions arise or additional text is received.

This multiplicity of entries may strike one as bureaucratic but is not, years of experience have shown that none of these entries can be dispensed with and that it is better in this respect to have too much rather than too little.

The intercepted message must get from the operator to the cryptographic section via traffic analysis section as quickly as possible. This is important. Even in peacetime one must not overlook the fact that in critical cases a few minutes lost by some fickle delay can never be made up for and may have catastrophic consequences. The same holds true for decipherment, it is better to hand over to evaluation every partially solved message than to wait until a more or less complete solution has been achieved.

Evaluation section will determine after mature but speedy consideration by tactically trained specialists whether a message is to be translated and included in the rupert or whether it is enough to enter certain data in the card file or whether a given message may be laid aside as of no consequence.

It is well to file messages which have been worked over between the rooms occupied by the cryptographic section and the evaluation section so that the former has them available for further work while evaluation can also get at them readily. It must be remembered however that the deciphered message is a top secret document and must therefore be kept under lock and key.

This form is perhaps the only one which passes through all four sections of signal intelligence and it is in the interest of everyone that the hand writing be good. Since the decipherer probably has the most time he should probably make his entries in printed letters, all the more so since reading a foreign language, e. g., Russian, is difficult for those not well versed in the language.

b. Forms for letter counts and decrypted systems.

For the moment it is enough to know that in general a knowledge of the frequencies in a language, be it letters, digrams, trigrams, syllables or words, is the "short multiplication table" of the analyst. Beginning with the simplest substitution system where the letters of the plaintext, i. e. of the language involved, are replaced by different combinations of letters or digits and continuing through the most complicated combined systems, the study of frequencies during various phases of analysis plays a great roll, even though it be only to pick out single methods of encipherment from the total number theoretically possible.

The forms for frequency counts are set up differently according to their purpose and manner of use. Theoretically there should be forms for the study of all possible digit or letter combinations but years of experience have shown that we can pass by various unlikely combinations and that several forms are adequate for the study of a number of combinations.

The following combinations occur in the cryptography of almost all countries:

Numerical texts:

Groups, consisting of one digit	= Z	= 1Z
" " " two digits	= ZZ	= 2Z
" " " three "	= ZZZ	= 3Z
" " " four "	= ZZZZ	= 4Z
" " " five "	= ZZZZZ	= 5Z
" " " six "	= ZZZZZZ	= 6Z

Letter texts:

Groups, consisting of one letter	= B	= 1B
" " " two letters	= BB	= 2B
" " " three "	= BBB	= 3B
" " " four "	= BBBB	= 4B
" " " five "	= BBBBB	= 5B

Mixed texts:

Groups consisting of one digit and one letter = ZB

Groups consisting of one letter and one digit = BZ

Mixed three place groups = BBB,BBZ,BZB,ZBB,ZZB,ZBZ,BZZ,ZZZ

Mixed four place groups = BBBB,BBBZ,BBZB,BZBB,ZBBB,BBZZ,BZZB,ZZBB,BZBZ,

Mixed five place groups = ZBZB,BZZZ,ZBZZ,ZZBZ,ZZZB,ZZZZ
32 possible combinations in all.

Note 1) Z= a single digit,
B= a single letter,

Note 2). Mixed groups of 3, 4, and 5 are rather rare since transmission of such combinations is relatively difficult and gives rise to many errors.

Note 3). 4 and 5 place mixed groups are generally transpositions (Polish border guard before 1937) or poly-alphabetic or machine systems following the expanded Treitheim method.

For the frequency study of the 10 digits no particular form is required, the same holds true for the individual letters (in Russian 31 without the hard sign or apostrophy).

The form sheet for dimono frequencies for all the 100 possible combinations (00--99) and those for all 961 possible letter combinations of the Russian language are similar in structure and use. The coordinates are always read in the sequence left hand column -- upper row [side-top]. (See appendices 5 and 6). The bigram to be entered is marked in the appropriate cell by a vertical stroke. It is well to make the 5th, 10th, 15th, 20th etc. stroke diagonally through the 4 preceding since this facilitates checking and counting. These forms are used also for frequency

count of 4-digit or 4-letter combinations when there is homogeneous cipher material which upon cursory examination shows only a limited number of different 4-digit or 4-letter groups which are repeated. When using the forms of appendices 5 and 6 for counts of 4 place combinations, the last two elements of the group are entered in the cell defined by the first two.

When studying three digit groups (i. e. trinome frequencies) a form with 1000 cells is needed, with the form (appendix 7) the order of reading is the upper row (hundreds) -- left column (tens and units) [top-side].

For three letter groups a similar form is not practicable (the 961 possible digraphs would have to be entered in the left hand column), the form in appendix 6 is used and the third (final) element is entered in the cell defined by the first two.

The form in appendix 8 serves for a frequency count of 4-digit groups, the thousands and hundreds are indicated by the vertical and horizontal marginal coordinates, the heavily framed cell thus indicated is divided into 10 small cells corresponding to the tens in the sequence 0, 1, 2 .... 9, reading from left to right first the upper then the lower row. The unit element of the 4-digit group is entered in the small cell. It is quite possible to use the form of appendix 7 for a 4-digit count, in this case the unit element is entered in the cell found by the three coordinates (thousands, hundreds, tens).

For frequency studies of 5-digit groups it is best to provide a book with 100 forms like appendix 7. The 100 dinomes formed by the ten thousands and thousands correspond to the 100 pages of the book, the final trinome (hundred, tens, and units) is marked by a horizontal stroke in the appropriate cell of the appropriate page.

For 5 letter groups 100 pages of the form in appendix 4 are bound together and the 5th (final) element of the 5-letter group is entered in the cell located by the hundreds and tens.

A statistical count of several-place mixed groups is rarely necessary. Due to the very many possible combinations difficulties are encountered. The first thing is to determine the ratio of letters to digits. As will be seen from the description of the method important deductions can be drawn from this. The frequency of the various conbinations can be determined, without regard for the value of the individual elements of the groups, and from this clues may be obtained for further work. In any case there are no forms to take care of all the theoretically possible combinations of mixed groups and any statistical studies will have to be adapted to the individual case.

During the war with Russia it was sometimes necessary forreasons of expediency to provide special forms but since these were designed only for special cases we may omit any description here.

The form for indexing all values of digit groups which may occur contain all the 100 dinomes in chronological (terminologic) sequence, with space for entering each dinome. This is a double sheet printed on both sides so that for a study of 3-digit groups 5 (5x2x100) such double sheets are required, for 4-digit groups 50 (50x2x100) and for 5-digit groups 500 (500x2x100). Since in binding these double sheets the top and bottom page are separated and remain unused we need 6, 51 and 501 form sheets respectively (See appendix 9).

It may be remarked that such statistical studies of 5-digit groups are rare and when one is made, this may be done on the forms (appendix 11) intended to be used as the actual code pages. Since these lines are ruled close and 4x100 bigrams are accommodated on one double sheet, the thickness of the book required is reduced from 501 to 251 double sheets.

The index (Kettenstatistik), as the description of methods of decipherment will show, serves both for a study of frequency and also for a study of the tendency of individual cipher elements to link together, whether these elements turn out to be letters, numbers, bigrams, digrams, syllables, words, concepts, or punctuation. Indexing is used primarily when solving non-alphabetic codes after the encipherment has been removed.

Entry in the index (appendix 9) is as follows:

We assume that a non-alphabetic 4-digit code, from which it has been possible to remove the encipherment (additive, transposition, or substitution) is to be subjected to statistical study in order to determine the meanings. Why such treatment is necessary will not be discussed here, the description of the method will clarify the point.

Theoretically a 4-digit code has 10,000 different possible groups, i. e. 51 forms like that in appendix 7 are needed in order to enter all individual groups. After these forms have been fastened together, the double pages are numbered serially 00 to 99.

Let the text read: 7414, 2893, 5008, 6873 .....

We open to page 74 and enter in the space opposite 14 the complete following group, i. e. 2893. Then on page 28 in space 93 we enter 5008, etc.

No similar form can be prepared for indexing letter groups because the 961 theoretically possible 2-letter combinations of the Russian alphabet cannot be accommodated on a double sheet and leave room for the entries. Here the form in appendix 10 is used but if it were ever necessary to treat 4-letter groups in this way some 1350 sheets would be required. It may be remarked that in 12 years experience with Russian military and political systems this has never been necessary and if we recall that the most extensive Russian code today had some 23,000 groups, it seems unlikely that any code will appear i n the near future — unless perhaps for diplomatic or economic use — with $31^4 = 923\,521$ groups. This is even more true for 5-letter groups.

For entering recovered groups during the breaking process sheets like those in appendix 5 or 6 are used for 2-place systems and sheets like that in appendix 7, or 31 bound sheets like appendix 6, for 3-place systems, i. e. the same forms as are used for statistical counts. For 4 and 5-digit groups the form shown in appendix 11 may be used appropriately and for 4 or 5 letter groups the necessary number of sheets like appendix 9 or 10. In the detailed description of methods of decipherment, the main portion of this book, the practical use of nearly all forms described here will be met so that their suitability will be indicated at that point.

3. Sorting, logging and preliminary study of cipher messages.

Looking back over the experiences of the years prior to and during the war it must be stated that too little care was devoted to the sifting and the ensuing sorting, logging and preliminary study of the intercepted traffic and that this preliminary work was done under quite erroneous assumptions.

Message sorting, or actually message counting, in the former German signal intelligence served primarily to control the capacity of the several intercept units and to stimulate their ambition and encourage a competition which rarely had any beneficial effect on the work itself. The increasing number and total of messages intercepted might impress an outsider but for the specialist himself more value attached and attaches to the quality than to the quantity of the messages.

The actual assignment of this subsection of the cryptanalytic section which we may call Logging (Registratur) is very extensive and varied. The log section is in the first place the connecting link between traffic analysis and through this with the receiving station on the one hand and the actual cryptanalysis on the other. In the second place it has the duty of sifting incoming traffic from very many points of view, of arranging it and logging it and in the third place passing it on after preliminary study to the analytic section whenever there appears to be a sufficient quantity of homogeneous material. The log section must always know which groups of traffic can be decrypted and read currently, which have been worked on, which are urgently needed to advance analytic work, which have valuable contents, especially urgent reports etc., which are practice messages, etc.

When these positions were filled with untrained or only poorly trained people without practical experience, it was not surprising that the demands to be made of this subsection of the cryptographic section could not be met. Toward the last, efforts were being made to correct this situation but it was already too late since none of the few specialists could be spared for this task.

The head of the log section and, if possible, another member who will at the same time serve as deputy must be analysts. Linguistic ability is not absolutely essential in this position. Obviously the preliminary study of traffic in unknown systems is a very difficult and responsible task, one which when performed correctly and conscientiously not only saves time but relieves the cryptanalyst. The analyst in the log section should and must heed the advice and opinion of those who will work on the material later and in case of need he must by his guidance and counsel exert an influence on traffic analysis section.

The following discussion of the complex task of a log section is based on the treatment of Russian cipher material but in the main is applicable generally.

Traffic received from the intercept station via traffic analysis is sorted according to group structure, duplicate messages are clipped together and marked as such but are not to be destroyed under any circumstances. Making use of information available in the log section respecting lines and networks, plans, call signs, message characteristics, etc. and data from the cryptographic section itself, the traffic in systems which have already been broken can be sorted out and delivered to the workers at once. The same holds true of material which, although not finally cleared up, is in an advanced stage. Practice messages, which are no rarity during relatively calm periods even in war, are sorted out and laid aside after being passed on by one or more analysts. The arrangement of the remaining messages, within the individual group lengths, calls for analytic skill and abundant experience. It is a question of getting homogeneous material together, be it on the basis of obvious group combinations,

of operational symbols, call-signs or wave-lengths, like or similar message headings, message numbers, key groups or indicator groups. In addition this material must be logged and studied when there is enough to warrant study. This study is not an attempt at decryption but merely aims to determine whether decryption is possible and probable. Such study may show for example whether a group of traffic is enciphered by a relatively simple substitution, whether an additive or a transposition is involved, or whether the amount of traffic available in a given group is still too small to warrant an attempt at decipherment.

Very important, primarily for unsolved transpositions, is the search for partial and complete compromises. The values of these will be discussed in detail later. Finding such compromises is only possible if the incoming messages of any group of material are carefully recorded. This is best done by lists which are filed with the group and contain the following information for each message:

1. Intercept number of the message.
2. Message number in the heading.
3. Number in cipher text.
4. Date and time of interception.
5. Tactical time (from the heading).
6. Indicator group (s)
7. Cryptographic data.
8. Group or element count.

In each case one must consider whether such exact and relatively time-consuming records are needed for individual messages of a group. The decision must rest with the head of the logging section or be made after consultation with other specialists. It may happen that such careful logging of a group of messages will not be made until a certain amount of like traffic is available.

If the log section has recognized by its preliminary study that a group of material is promising and if its opinion has been confirmed by one or more specialists of the cryptographic section, then the log section through its contacts with traffic analysis must see to it that additional messages of the group are intercepted if this be possible. This influencing of the intercept stations via traffic analysis must be handled primarily by the log section. It must be remembered that the intercept stations, the individual operators, without precise, closely defined directives and instructions for their search will hear on a definite wave band, indeed on a specified frequency, that which is relatively easy to get and comes in strongest. If we further consider that at present radio has become the common property of all nations, it will be obvious that in individual wave or frequency ranges numerous stations will lie close to one another and that the operator, in case he has no precise instructions, can choose among these or can copy messages of all conceivable circuits falling within his band. The operator cannot be chided for this, it simply happens that, where there is a choice between easy, hard and very hard, people will always prefer the easy. Quite apart from that however the intercept operator is not in a position to determine the worth of worthlessness of a cipher message. In many cases traffic analysis can give guidance,

assuming that from its evaluation it has arrived at certain deductions, hunches or assumptions without textual clarification on the part of the cryptanalytic section. However this will rarely be the case with new systems. Here then only the cryptographic section, and within this the log section, is competent, therefore it is from this section that directions are to be expected and demanded. Such a decision is only possible if the log section has been able to form some conception of the new traffic, i. e. has carried out its preliminary study. Since under normal circumstances the complexity of structure increases with the higher echelons, i. e. an army group will not have any simple system, a regiment on the other hand will not employ any very complicated additive encipherment, this fact permits certain inferences regarding a system once the traffic has been subjected to a preliminary study.

This preliminary study is, as already stated, a step preparatory to cryptanalysis itself; as far as statistical work is concerned it employs the same methods and it will be described in detail in its proper place.

4. Hollerith methods and mechanical aids.

The following observations will hardly be intelligible to the layman without previous study of part 1, primarily of the cryptographic systems. Consideration of the problems of the Hollerith methods and the mechanical aids from a purely theoretical standpoint would be quite meaningless. It is also recommended that the reader compare details of this chapter with part 3, methods of decipherment, in order to elucidate anything which may not yet be clear.

The Hollerith method, or as it is also called in Germany the punch card method, did not find recognition as a mechanical machine aid for various phases for cryptanalytic work until the beginning of the war 1939/45. Then it gained in importance from year to year and at the end had become indispensible. In spite of this or perhaps precisely because this method has become so important for study and sorting, in lay circles and also in circles coming in indirect contact with signal intelligence or its results the erronous impression has arisen, that the Hollerith machine as such is a kind of mechanical deciphering device, i. e. that it can replace human mental effort. This is in no wise true. The Hollerith method merely replaces and speeds up the investigations which are considered correct or important by the analyst, i. e. by the human mind, it performs mechanical tasks exactly and with a saving of time, tasks which formerly would have to be performed by a number of clerical assistants.

Among the large number of things the Hollerith machines can do only those will be mentioned here which are directly connected with the work on Russian cipher material.

The real reason for employing Hollerith machines was the appearance of difficult additive encipherments with practically endless additive sequences. This was all the more necessary when the Russians later began disguising the indicator groups which up to that time had given some clue as to the relation between various messages of a series.

For dealing with messages enciphered with additive the primary need is for a calander of differences or, better said, a catalog of differences, quite immaterial whether the enciphered code itself is known or is yet to be recovered. As is clear from the description of the systems in part 1,

the differences formed from two frequent code groups, are themselves relatively frequent. These differences do not change if both groups are enciphered by one and the same additive group. On the basis of a certain number of frequent differences it is sometimes possible after lining up the individual columns of groups to reduce them to a common denominator (Nenner) and to break into the system if it is unknown. When the code itself is known, as was frequently the case in the war against Russia through fortunate circumstances, the procedure in laying out a difference catalog is as follows:

After the most frequent code groups have been picked out on the basis of observations or by Hollerith methods and have been subdivided into several classes according to their frequency, the difference catalog can be computed with the aid of Hollerith machines.

Example of a plan for Hollerith differencing (Russian code with 10,000 groups)

Class 1	(,)
	(.)
"Extremely frequent meanings"	И
	В
	С
	Х

	О
	А
	(-)
Class 2	(:)
	НА
"Very frequent meanings"	ПРОТИВНИК
	КОМАНДИР
	ПОЛК
	НАЧАЛЬНИК
	СТРЕЛК. ДИВИЗИЯ

Class 3	Е
	У
	НЕ
	ОТ
"Frequent meanings"	ДО
	ШТАБ
	РАЙОН
Class 4	Т
	ПО
	АРМИЯ
	ПЕХОТА
"Rather frequent meanings"	РОТА
	АВИАЗИЯ
	1
	2
	3
	4
	5
	6
	7
	8
	9
	0

For the code groups, i. e. the numbers equivalent to the plaintext, cards are punched and these are differenced as follows:

Differences formed from	Number of differences
Class 1 with itself	15
Class 2 with itself	45
Class 1 with class 2	60
Class 1 with class 3	42
Class 1 with class 4	96
Class 2 with class 3	70
Total	328

The difference catalogue computed by the above plan would therefore contain 328 differences.

Another very important step is lining up, i. e. superimposing in phase the various messages of an additive series. In this case two messages, punched in tape, are slid by one another and the differences of all superimposed groups are computed in every position by the Hollerith machine. In many cases the correct position of the messages relative to one another will be the one showing the largest number of frequent differences. This method need not always prove successful, it is based on pure probability and represents merely an experiment. However if it is possible to line up two messages in this way, the possibility of a further line up with each message is increased manifold, because now sliding a third under those already lined up will give twice as many differences in each position.

In connection with this manipulation the search for repeats may be mentioned. Precisely with additive encipherments, especially where 5-digit code groups are enciphered by additive, repeats are very often the key to an alignment and so to a possible break.

Let us assume for example that the 18th group of a message in 5-digit groups corresponds to the 27th group of the second message and that the 34th group of the first corresponds to the 43rd group of the second. In this case, since the interval 18 to 34 is the same as that from 27 to 43, the probability that the line up is correct is almost 100%. Hence the 18th group in message 1 should stand above or below the 27th group in message 2, the 34th group in message 1 would then automatically stand in the same column with the 43rd group of message 2.

Like the search for repeats, the search for parallel passages can also be made by Hollerith machine. Here however it is a question whether the time expended in punching up all the groups of numerous messages and in the ensuing machine operations is not greater than the time required for manual indexing which cannot fail to disclose every parallel passage and repeat.

Among the general aids already mentioned are a number which owe their origin to Hollerith methods. We need only mention the lists of place names and family names read backwards.

The processes mentioned do not by any means exhaust the possibilities of service by machine methods. But the examples cited should suffice to document the appropriateness and elasticity of these methods while at the same time they show that the machine cannot be credited with creative ability.

If it is not to expand beyond all bounds, the section "mechanical aids" must be limited to a discription of the most important and really serviceable apparatus of this nature and cannot enter into a discussion of the pros and cons respecting construction and use of many smaller devices which may be useful for a time. As already mentioned in the introduction to the chapter on "general aids", the construction and use of numerous mechanical aids often serve as a plaything or "individual hobby" rather than to simplify and speed up the work. In this connection we may point to the so called encipherment slides ("Überschlüsselungsschieber) which were often very elaborate, made of rare wood and even carved or painted, which were supposed to facilitate finding or setting up an encipherment. In most cases a simple sheet of paper inscribed with the substitution sequences

involved and folded to correspond with the indicator groups yielded the encipherment in question.

On the other hand various little mechanical aids cannot be dispensed with, these are really quite simple things, for instance strips or rods of ivory or thin enameled metal for solving transpositions or polyalphabetic substitutions. Grille overlays are likewise absolutely necessary, no matter whether dealing with the rare revolving grille or with the Raster system of the type used by the British airforce 1939/41. No objection can be made to these little mechanical aids, they will always find application and have to be constructed.

During the course of work on additive encipherment, in particular when lining up, someone hit on the idea of writing the messages on tapes and sliding these against one another so as to be able to compute the differences better in each position. The strips were gummed on the back and when aligned were cut message by message into sections of ten groups each and pasted one below the other in phase. To produce these tapes a teleprinter was used which was cut off from the communications net and served solely for this purpose. After several messages were lined up, the break-in i. e. the solution of various columns, resulted by use of the difference catalog. These breaks were expanded as far as possible to the right and to the left on a linguistic basis. The expansion could be assumed to be correct when all messages gave logical, intelligible plaintext from column to column. It did happen however that some columns, even with sufficient depth (several messages in phase one beneath the other) neither showed known differences nor could they for the moment be extended on a linguistic basis.

For the solution of such refractory columns a device was made for reducing all messages of a column automatically. This will be described as conclusion of this chapter. (Compare appendix 12)

In a metal box are mounted 5 shafts (a). On each of these shafts are several freely rotating wheels, all at the same heighth. On the lower ends of the shafts, which project through the metal box, are knobs (b). If these are moved, the free movement of the wheels on the shaft is blocked and the wheels now turn only with the shaft. All wheels (c) are inscribed with the digits 1—0, windows in the box allow one digit of each wheel to show.

The gadget is used as follows:

The upper series of wheels is set on 00000. The five wheels (inscribed with digits) of each row are set to correspond to the 5-digit groups of a "refractory column". If the position of the shafts is changed by turning the knobs below until in one message the code group appears which, on the basis of context, may be assumed to be correct, then the wheels for all the other messages have automatically turned the same distance. The top row shows the symbolic additive of the additive sequence. This procedure can be repeated until a position is found which yields proper textual continuity for all messages.

5. Card catalogs.

Although the card files are treated last in this paper they are by no means the least important of the general aids. There is another reason for this. These files are an aid to the cryptographic section and perhaps to

an even greater extent to the evaluation section and have been maintained since 1939 almost exclusively by the latter. For this purpose use is made not merely of results of our own cryptanalytic organization but also of all news, reports and pieces of information that may come in through monitoring the press and broadcasts. Moreover evaluation also works in, when appropriate, reports of interrogations of agents, spies, prisoners and deserters. Captured documents sometimes helped to complete the card files. However it must be remarked that what does not result from decrypted messages is taken up into the signal intelligence card files only under reservations and is not therefore regarded as absolutely sure. To differentiate facts from assumptions, the cards dealing with dependable information are generally typed while unconfirmed reports are noted in pencil. For the same reason and to enable constant checking there is a space on all cards for an indication of the source and this space must always be filled in.

All cards are divided into two parts, the upper part containing what amounts to an evaluation of the lower part. This evaluation can be checked in any event against the exact word for word extracts below with statement of the source. This procedure has the good point that no room is left for fanciful deductions on the part of the individual and the statements on the upper part of the card can be accepted as fact.

The first and most important file, especially for decipherment, is the collection of names, primarily of names which have occurred in deciphered messages.

If we remember that the family name as such either as address or signature is perhaps the best point for analytic attack, it becomes evident to what an extent knowledge of the names of the most important military or political leaders of a given network can be of help in breaking a new code or a new encipherment when a change has occurred.

Appendix 13 shows a sample name file card. The card is adapted to the Russian language and has space on the second line for entering given name and father's name. It is to be recommended that the cards, at least as far as the name is concerned, be filled in with Russian letters, the same name maybe entered transcribed into ones own language in parenthesis.

Every occurrence of one and the same person, insofar as the name appears without comment within a brief space of time, is entered on the back of the card with source and date. In this way it is possible to supplement the information on the front and likewise to fix the time when this person last appeared.

The card in appendix 14 serves for recording all troop units of the army, airforce and navy with their momentary subordination to higher units and of military and political offices with information as to their make up and what they belong to. Every change of position, employment, assignment or use is noted here with date and source.

The card for abbreviations (appendix 15) gives the abbreviations both in Russian letters and our own. It often happens that a new abbreviation cannot be interpreted at once or that any interpretation is based solely on ones own reflection and deductions. In that case it is only noted in pencil on the upper part of the card while the content from which it is taken is typed definitively on the lower part.

The card in appendix 16 is valid for all types of craft whether war ships or merchant ships, planes, tanks or automotive vehicles. From the entries on the upper part of the card it must be clear what kind of craft it concerns, on the lower part the entries which are not applicable are stricken out.

If a type of submarine is to be described for example then from the group "Höhe, Tiefgang" the concept "Höhe" would be stricken out and the concept "Tauchtiefe" would be filled in in detail.

The card in appendix 17 is used for factories, plants, concerns, trusts, unions, warehouses etc.

The three different suggestions for entering the designations are by no means superfluous in view of Soviet habits. A corresponding entry might appear as follows:

Designation: ГОРЬКОВСКИЙ АВТО ЗАВОД

Abbreviation form: "ГАЗ"

More particular designation: ЗАВОД ИМЕНИ МОЛОТОВА

The form allows for any existing branches and defines the subordination to the corresponding ministry, trust, concern, or union.

Here too it is very important to keep the entries on the back current and not be content when the front of the card is filled.

The five sample cards described cover essentially all that is required from the cryptographic and for the evaluation section. For carding additional useful information, for example arms and implements, blank cards of the same size but in different colors were available which had to be filled out according to the purpose they were to serve.

In the former German signal intelligence service the card catalog was kept in the German language in spite of valid arguments to the contrary. Only in the last years of the war was it possible to have at least family names and abbreviations entered also in Russian letters. The reason was that content evaluation was composed of persons who, quite apart from the fact that they were not equal to their own assignments, very rarely had any command of the Russian language. Up to the war signal intelligence was a stepchild of the German armed forces without "glorious" tradition and without obvious successes, hence it was not surprising that officers with linguistic training and tactical ability were considered wasted on this branch and that in place of such men subordinate officials of the upper middle grade, i. e. Inspektoren and Oberinspektoren, tried their hands at content evaluation. When at last the value of signal intelligence as the surest source of intelligence had been recognized, time, the unfavorable military situation and the dearth of personnel imposed a veto on any reorganization, so that with slight changes no essential improvement could result.

This inadequate handling of the files, which did not meet requirements, forced the cryptanalytic section to help itself. It set up supplemental files. It may be remarked that the card files, in particular with the originally very small cryptographic section of the army, were originally exclusively an aid for the cryptographic section and the needs of a limited content evaluation were also taken into account. After the creation of an independent evaluation section on a rather large scale, primarily at the central cryptographic section in Berlin (Horchleitstelle), the cryptanalytic

section was able to dispense with most of the card files. However in the course of time, due to the increasing difficulties both in solving messages and in identifying circuits and net works, a special card, called a "Geheimschriften - Steckbrief" [warrant for arrest of cryptographic systems] was developed which was used with little variation in form by the army and the airforce. This "warrant of arrest" combined the data from various types of card files and was adapted to the exclusive needs of the cryptographic section.

Appendix 18 shows such a "Geheimschriften - Steckbrief". The sum of the entries, assuming they are always up to date, gives for any system in use or superseded full information regarding the area of use, troops units mentioned, persons mentioned, etc. All details concerning pure cryptanalysis are likewise noted; identification with circuits and networks formerly read or with modified similar systems previously employed is possible.

In this folder is filed the system as such with all encipherments, method of decipherment, reports and all other details. These "warrants" are treated as top secret documents and are the most essential basic documents for the work; collectively they are handled according to the motto "divide et impera" and they are kept in the safe of the head of the cryptanalytic section and administered by him personally.

Regarding these "warrants" we may say that the numbering of the cryptographic systems corresponds to the number of the warrants and that the first digit of the number gives the number of digits or letters of the cipher group in the system. In the German signal intelligence all

2-place systems were numbered from 2001 to 2999, 4-place systems from 4001 to 4999.

The chapter on general aids may be concluded with this description of the card index system in general and of the different cards in particular. Even the layman will understand that the creation of these documents required a long time and that the development was by no means concluded with the state of things at the time of the capitulation. Likewise it must be remembered that every state, every country of institution which maintains a signal intelligence with associated cryptanalytic activity has developed similar but yet different aids corresponding to its own mentality and that the decipherment of diplomatic and economic systems calls for far more material.

No attempt is made within the limits of this paper to describe the office set-up of the cryptanalytic section and the evaluation section, this can be deduced readily from what has already been said. Naturally all technical innovations such as good lighting, typewriters with Latin and Cyrillic chracters, long and short carriage, good communications, i. e. telephone or microphone layout, teleprinter and secret teleprinter, Hellschreiber, radio broadcast, speech scrambling and descrambling equipment, are necessary for smooth operation, likewise all writing and drawing materials and suitable furniture. As for the allocation of space the most important thing is to avoid too close crowding. All those who are expected to do real mental work must have ample room and a proper degree of quiet.

Experience has shown that for the cryptanalytic personnal, i.e. Those working on difficult systems, not more than two to the room is desirable while the so called assistants, i. e. those working on easy systems, those of medium difficulty or systems already solved, may be placed about six together in a correspondingly larger room. It is best that those working on one and the same system be able to sit near together. Secret and top secret documents must always be checked, if not by the chief then by some duly authorized representative.

SI unit:

receiver:

number:

radio operator:

to:

date: 19

frequency: (wave:)

strength of reception:

from:

hour:

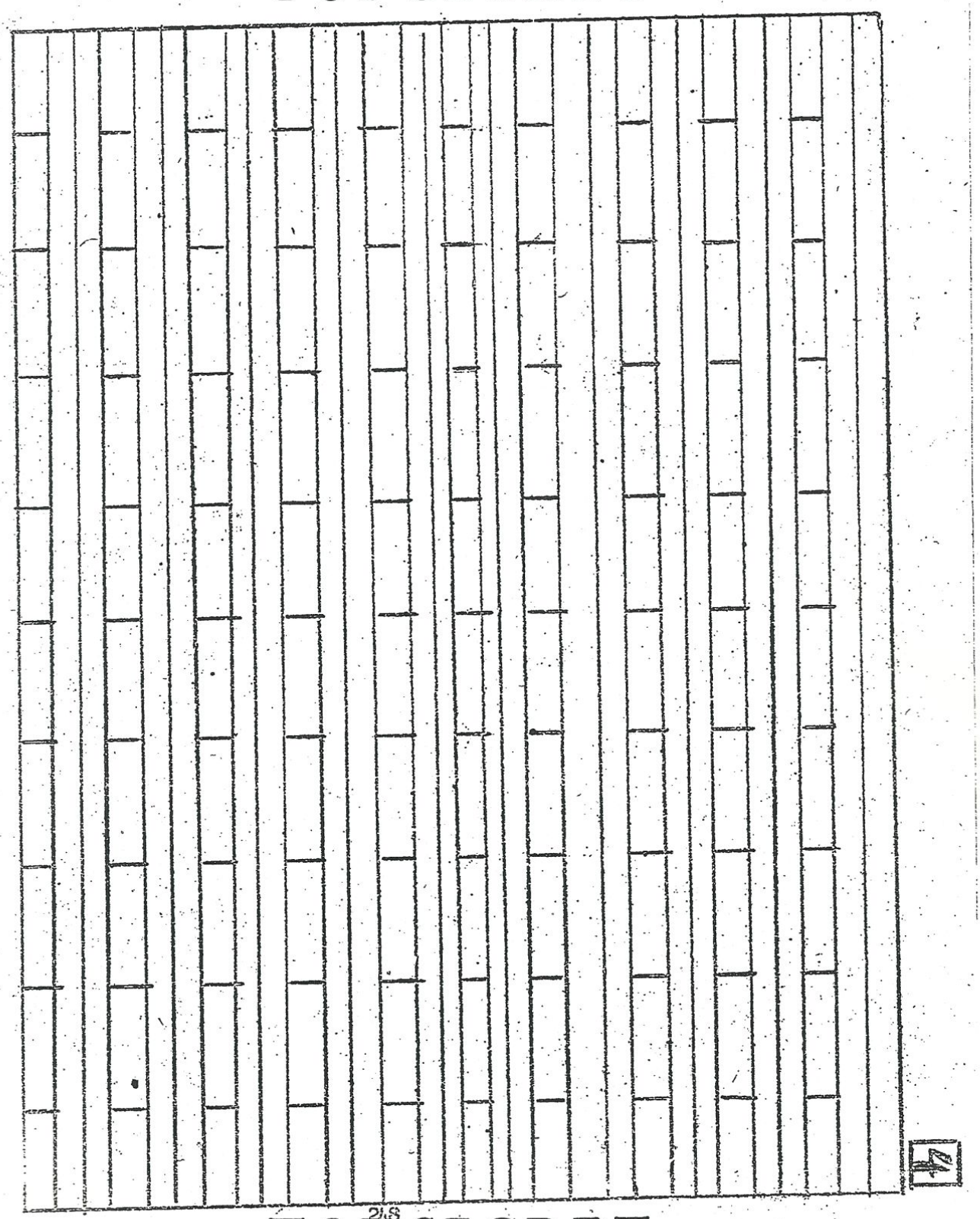
net work:

method:

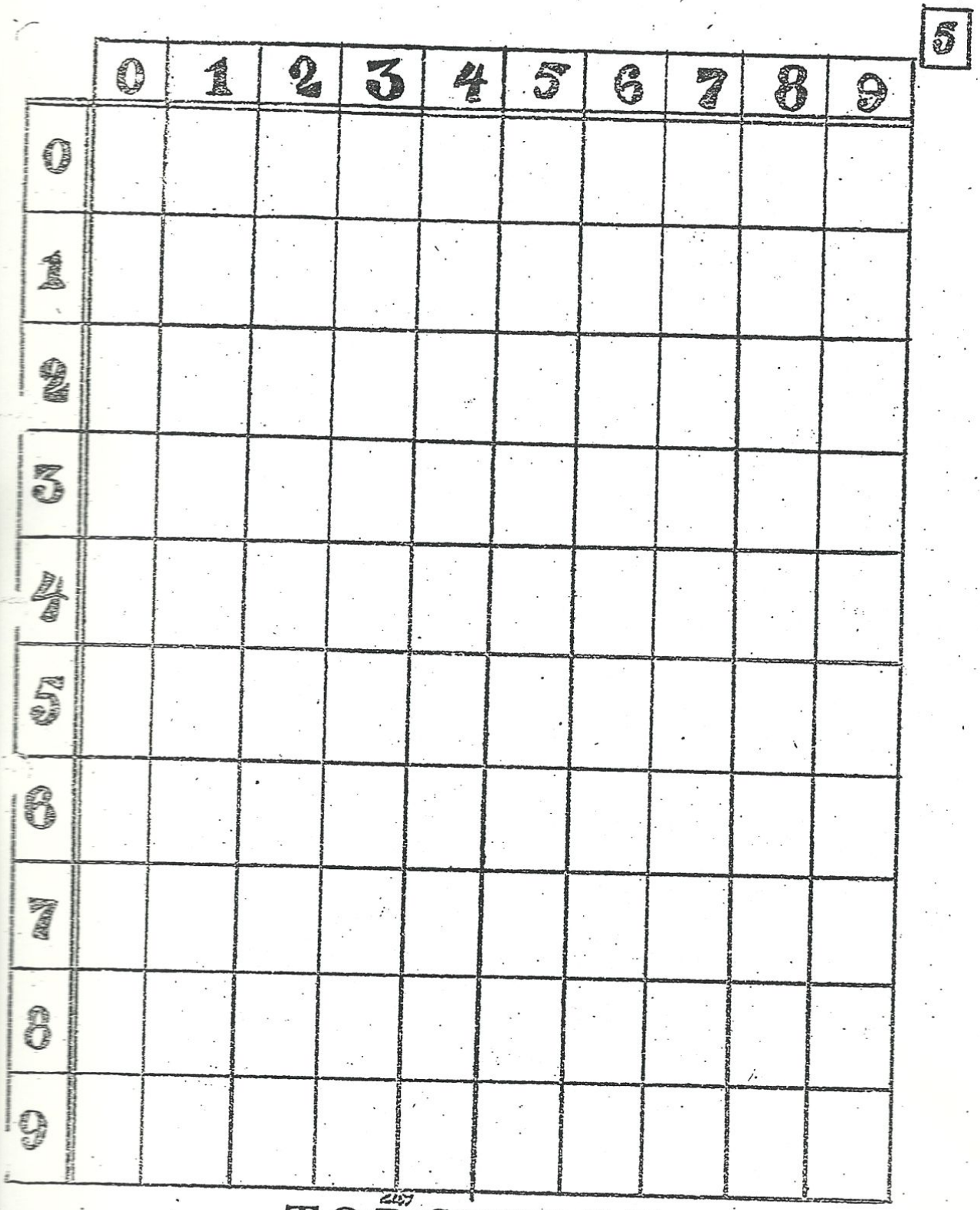
date when forwarded:

own number:

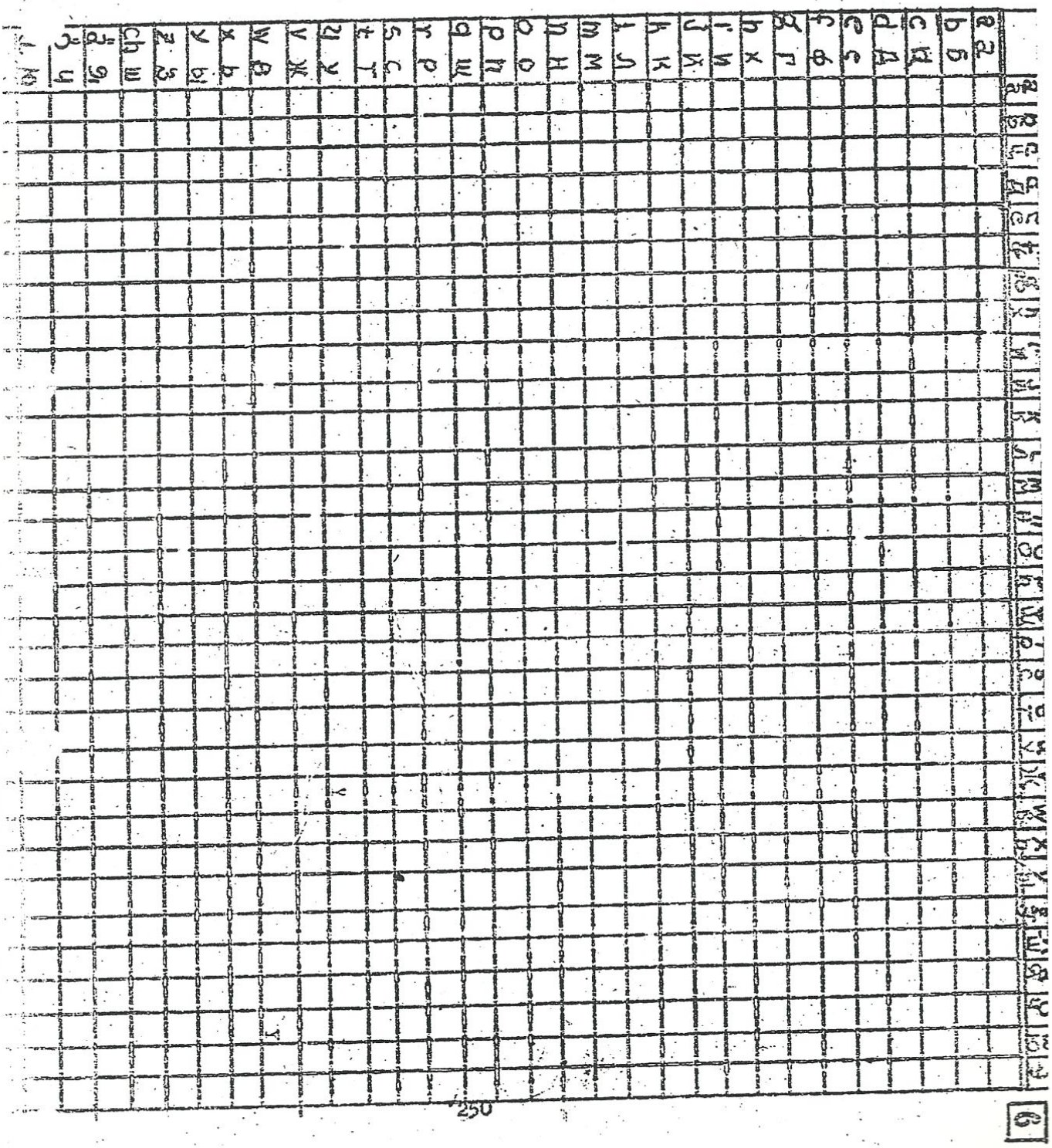
heading:



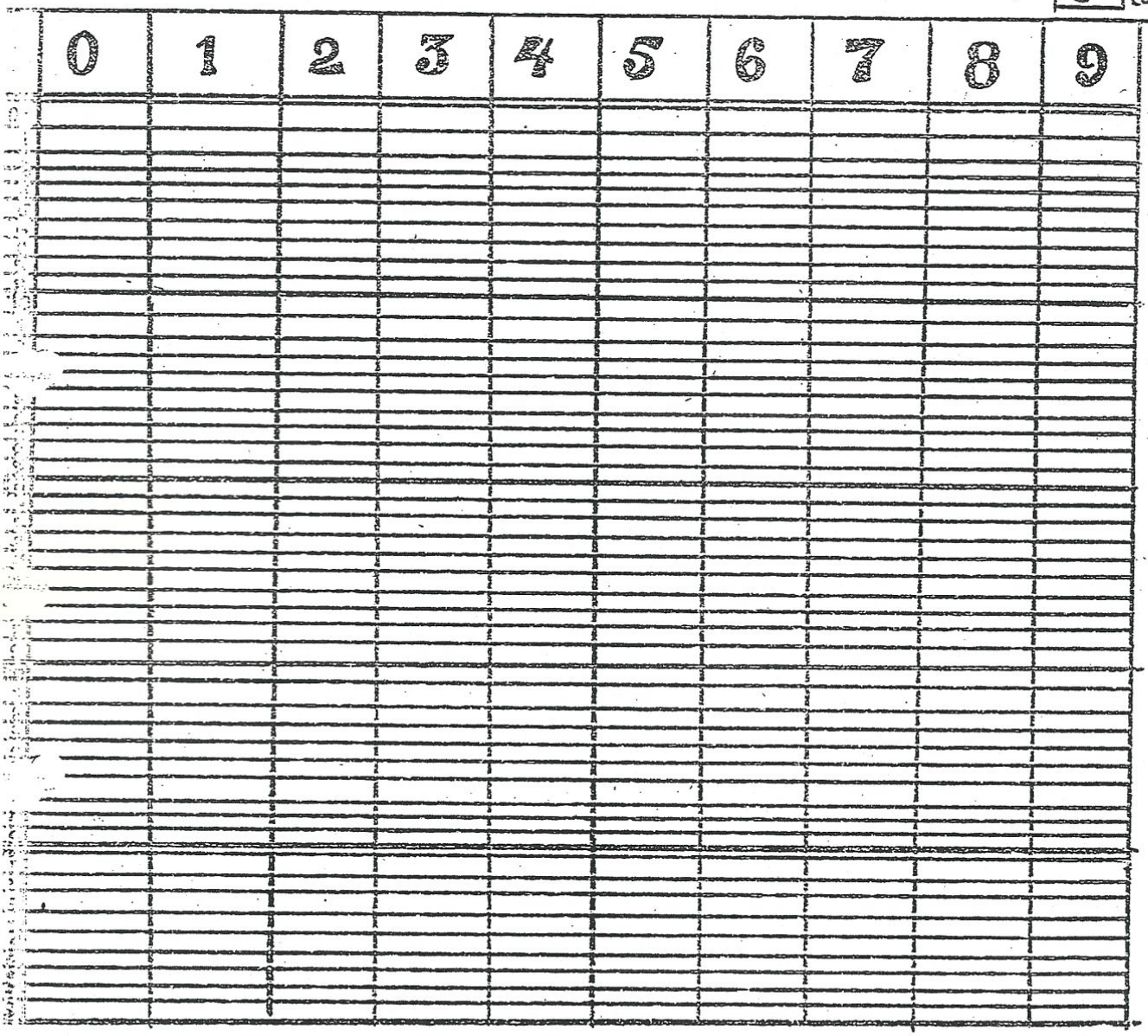
~~TOP SECRET~~



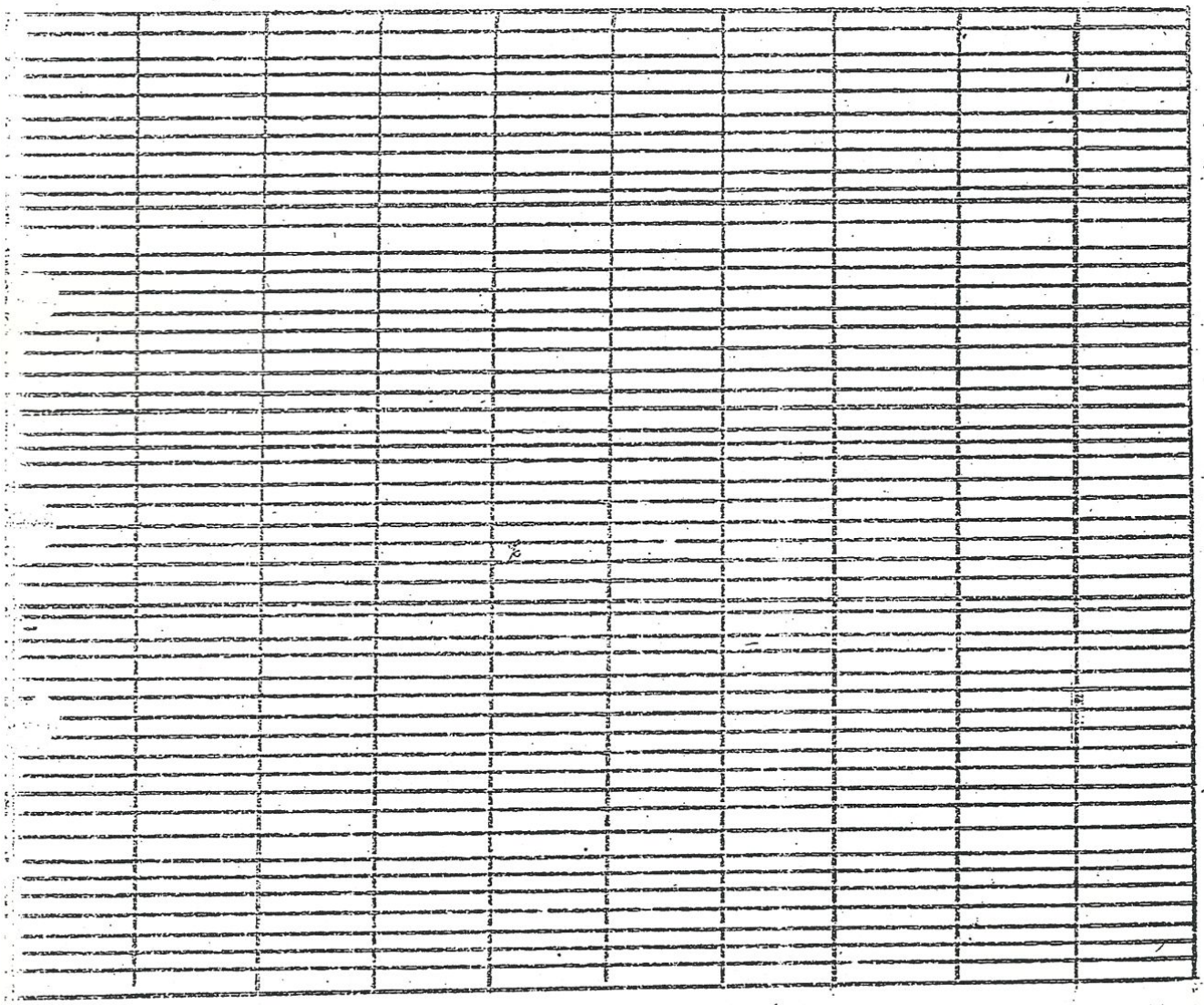
~~TOP SECRET~~

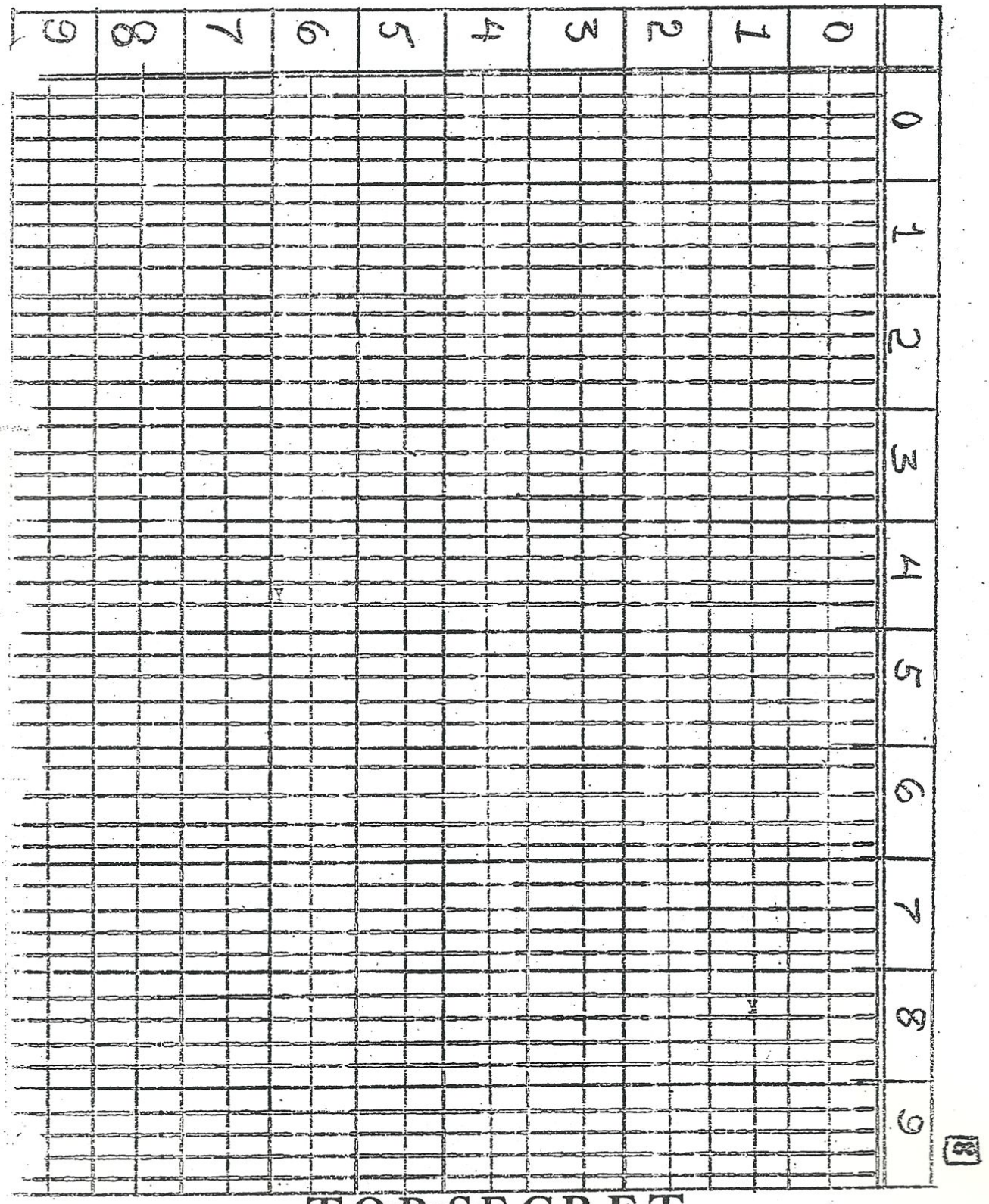


7 (a)



7 (b)




0 1 2 3 4 5 6 7 8 9
0 1 2 3 4 5 6 7 8 9

00	25
01	26
02	27
03	28
04	29
05	30
06	31
07	32
08	33
09	34
10	35
11	36
12	37
13	38
14	39
15	40
16	41
17	42
18	43
19	44
20	45
21	46
22	47
23	48
24	49

50	75
51	76
52	77
53	78
54	79
55	80
56	81
57	82
58	83
59	84
60	85
61	86
62	87
63	88
64	89
65	90
66	91
67	92
68	93
69	94
70	95
71	96
72	97
73	98
74	99

16

a

b

c

d

e

f

g

h

i

j

k

l

m

n

o

p

q

r

s

t

u

v

w

x

y

z

ch

ä

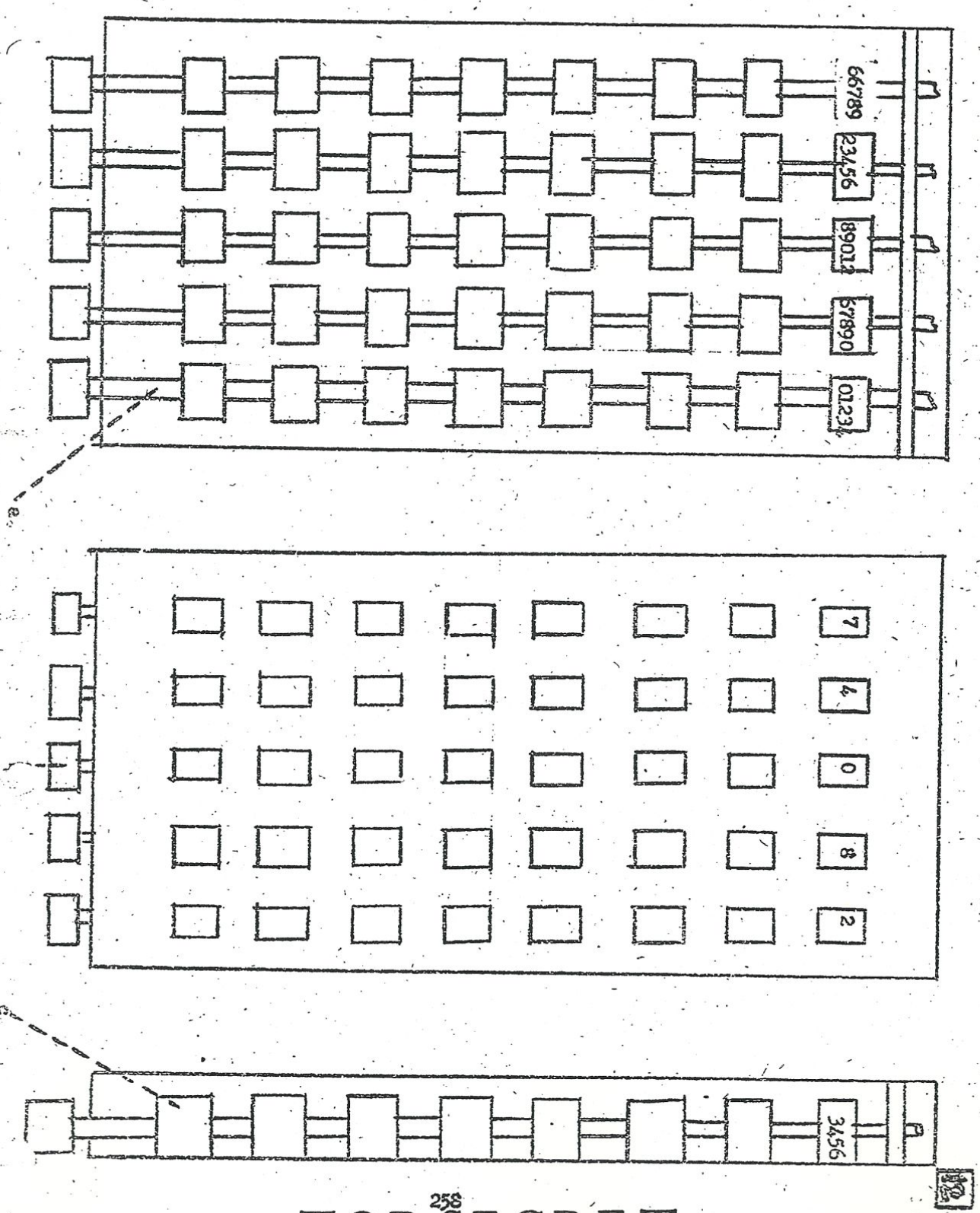
ö

ü

11

00	50
01	51
02	52
03	53
04	54
05	55
06	56
07	57
08	58
09	59
10	60
11	61
12	62
13	63
14	64
15	65
16	66
17	67
18	68
19	69
20	70
21	71
22	72
23	73
24	74
25	75
26	76
27	77
28	78
29	79
30	80
31	81
32	82
33	83
34	84
35	85
36	86
37	87
38	88
39	89
40	90
41	91
42	92
43	93
44	94
45	95
46	96
47	97
48	98
49	99

257


66789
23456
89012
67890
01234
7
4
0
8
2
3456

[front]
Last Name:

13

First Name and Fathers Name:

Rank:

Appointments and Duties:

Personal History:

Remarks:

[back]

DATE	SOURCE	CONTENTS (Additional Informations, Corrections, Changes Confirmations)

[front]

Unit or Administrative Headquarters:

14

Organization:

Remarks:

DATE	SOURCE	CONTENTS (Additional Information, Corrections, Changes, Confirmations)

[back]

DATE	SOURCE	CONTENTS (Additional Information, Corrections, Changes, Confirmations)

[front]
Abreviation
(English letters): (Russian letters):

Decoded meaning (original):

Translated meaning:

DATE	SOURCE	CONTENTS (Corrections and Confirmations)

[back] DATE	SOURCE	CONTENTS (Corrections and Confirmations)

[front]

Name or Type:

bject:

Purpose of Employment:

Remarks:

DATA	SOURCE
Year completed, Launching:	
Width, Span:	
ength:	
Height, Draught:	
Weight, Tonnage:	
Armament:	
Armor:	
Crew Number:	

[back] ADDITIONAL DATA	SOURCE
erformance or Capacity:	
umber of Engines:	
Type of Engines:	
Fuel Reserve Supply:	
Effective Range or Radius of Action:	
Maximum Speed:	
Cruising Speed:	
Landing or Diving Speed:	
Take Off Speed:	
Service Ceiling or Diving Range:	
Absolute Ceiling:	
Rate of Climbing (Maneuverability):	
Break-through Ability:	
Bomb Load, Ammunition Supply or Load Capacity:	
Type of Bombs or Hold:	
esigner:	
anufacturer:	

TOP SECRET

17

DESIGNATION MARKING:

ABBREVIATED FORM:

DETAILED OR ADDITIONAL DESIGNATION:

STRUCTURE:

263

SYSTEM DESIGNATION:

PURPOSE:

GEOGRAPHICAL LOCATION:

REMARKS:

[Note:--Back of card is ruled for:]

Date	Source	Contents (additional Informations, Corrections, Changes, Confirmations)

TOP SECRET

CODE IDENTIFICATION NO. [| | |]

Original designation: _____

Internal designation: _____

Structure of message groups: _____
Structure of code groups: _____

Limits of operation:
Unit, branch of service or MVD organization: _____
Organization: _____
Geographical location: _____

Time limitation from: _____ to: _____
Predecesor: _____ Code Identification No. [| | |]
Succesor: _____ Code Identification No. [| | |]

Structure of the code: _____

Reencipherment: _____

Identification groups: _____

broken by (coded by): _____
during the period of: _____ to: _____

dealt with and supplemented by: _____

Structure of messages: 18

Message characteristics:

Contents of messages:

Names appearing in the messages (in syllables)

Last Name	First Name, Fathers Name	Rank	Appointments and Duties	own No.

Units appearing in the messages

Unit, Administrative Headquarters, branch of service or MVD org.	Org.	Own No.

18

REMARKS: